PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-032664

(43)Date of publication of application : 29.01.2004

---

(51)Int.Cl. H04L 12/28
H04Q 7/38

---

(21)Application number : 2002-378650 (71)Applicant : TOSHIBA CORP

(22)Date of filing : 26.12.2002 (72)Inventor : ADACHI TOMOKO
TOSHIMITSU KIYOSHI

---

(30)Priority
Priority number : 2001395475
Priority date : 26.12.2001
Priority country : JP

---

(54) RADIO COMMUNICATION SYSTEM, RADIO COMMUNICATION APPARATUS, AND RADIO COMMUNICATION METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a radio communication apparatus which is capable of performing radio communication keeping the minimum security level by encryption predetermined by a communication group.

SOLUTION: In a communication system, a 1st radio communication apparatus belonging to the communication group, receives a connection request frame including a notice security level from a 2nd radio communication apparatus outside of the communication group. The 1st radio communication apparatus stores a proprietary reference security level of the radio communication group which is selected from security levels specified depending on a encryption method including non-encryption and its strength. The 1st radio communication apparatus generates a response frame which describes connection rejection to reject the connection to the 2nd radio communication apparatus or connection permission to permit the connection to the 2nd radio communication apparatus, comparing the notice security level and the reference security level, and transmits to the 2nd radio communication apparatus.

LEGAL STATUS [Date of request for examination] 09.06.2004
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1]
With the receive section which receives the 1st transmitting frame which has the 1st field where notice security level was described from the radio communication equipment besides a communication link group
The memory section which memorizes the criteria security level which was selected from the security level depending on the encryption approach including un-enciphering, and the strength of encryption, and was assigned to said radio group,
It reaches with the frame generating section which generates the 2nd transmitting frame which has the 2nd field where the connection refusal or connection authorization determined and determined is indicated [authorization / a connection refusal with the radio communication equipment besides said radio group, or / connection] in said notice security level as compared with said criteria security level.
The transmitting section which turns this 2nd transmitting frame to the radio communication equipment besides said radio group, and transmits,
The radio communication equipment belonging to said radio group characterized by providing.
[Claim 2]
Said criteria security level is a radio communication equipment of claim 1 with which it is selected from the 1st, 2nd, and 3rd security level, and said 1st security level is equivalent to un-enciphering, it is equivalent to the strength [the 1st] of encryption with a radio communication equipment, and said 2nd security level is characterized by the thing [in / in said 3rd security level / said 1st encryption] equivalent to the strength [the 2nd] of encryption in the 1st encryption.
[Claim 3]
Said frame generating section is the radio communication equipment of claim 1 characterized by determining a connection refusal if said notice security level is lower than said criteria security level, and determining connection authorization if said notice security level is not lower than said criteria security level.
[Claim 4]
The radio communication equipment of claim 1 characterized by said memory section holding the address and said notice security level of a radio communication equipment besides said radio group in said connection authorization.
[Claim 5]
Said 2nd communication link frame is the radio communication equipment of claim 1 characterized by including the 3rd field where the address which specifies said radio group was described.
[Claim 6]
It sets to the radio communications system which consists of the 1st radio communication equipment belonging to a radio group, and the 2nd radio communication equipment besides this radio group, and is said 1st radio

communication equipment,
With the receive section which receives the 1st transmitting frame which has the 1st field where notice security level was described from said 2nd radio communication equipment
The 1st memory section which memorizes the criteria security level which was selected from the security level depending on the encryption approach including un-enciphering, and the strength of encryption, and was assigned to said radio group,
It reaches with the 1st frame generating section which generates the 2nd transmitting frame which has the 2nd field where the connection refusal or connection authorization determined and determined is indicated [authorization / a connection refusal with said 2nd radio communication equipment, or / connection] in said notice security level as compared with said criteria security level.
The transmitting section which turns this 2nd transmitting frame to said 2nd radio communication equipment, and transmits,
The radio communications system characterized by providing.
[Claim 7]
Said criteria security level is a radio communications system of claim 6 with which it is selected from the 1st, 2nd, and 3rd security level, and said 1st security level is equivalent to un-enciphering, it is equivalent to the strength [the 1st] of encryption with a radio communications system, and said 2nd security level is characterized by the thing [in / in said 3rd security level / said 1st encryption] equivalent to the strength [the 2nd] of encryption in the 1st encryption.
[Claim 8]
Said 1st frame generating section is the radio communications system of claim 6 characterized by determining a connection refusal if said notice security level is lower than said criteria security level, and determining connection authorization if said notice security level is not lower than said criteria security level.
[Claim 9]
The radio communications system of claim 6 characterized by said 1st memory section holding said the 2nd address and said notice security level of a radio communication equipment in said connection authorization.
[Claim 10]
Said 2nd communication link frame is the radio communications system of claim 6 characterized by including the 3rd field where the address which specifies said radio group was described.
[Claim 11]
Said 2nd radio communication equipment is the radio communications system of claim 6 characterized by providing the 2nd memory section holding the address of said criteria security level and said 1st radio group.
[Claim 12]

It is the radio communications system of claim 6 characterized by said 2nd radio communication equipment transmitting the 3rd transmitting frame which has the 4th field where the 2nd notice security level was described to said 1st radio communication equipment when said 2nd radio communication equipment receives the 2nd transmitting frame which has the 2nd field where a connection refusal is described.

[Claim 13]

Said 1st memory is the radio communications system of claim 6 characterized by holding the encryption parameter relevant to the security level and encryption level which are supported with said 1st radio communication equipment, and selecting said criteria security level from this security level currently supported.

[Claim 14]

It is the radio communications system of claim 13 characterized by for said 2nd radio communication equipment transmitting the 4th transmitting frame which has the 5th field where encryption data are stored to said 1st radio communication equipment when said 2nd radio communication equipment receives the 2nd transmitting frame which has the 2nd field where connection authorization is described, and said 1st radio communication equipment compound-izing encryption data using said encryption parameter.

[Claim 15]

Said 1st transmitting frame has the 1st field where two or more notice security level currently supported with said 1st radio communication equipment was indicated. Said frame generating section compares each of said notice security level with said criteria security level. The radio communications system of claim 13 characterized by determining a connection refusal if said all notice security level is lower than said criteria security level, and determining connection authorization if one of said the notice security level is not lower than said criteria security level.

[Claim 16]

Said notice security level is the radio communications system of claim 6 characterized by being equivalent to the greatest level in the notice security level which said 2nd radio communication equipment supports.

[Claim 17]

The radio communications system of claim 6 which is the 3rd radio communication equipment besides said radio group, and is characterized by providing further said 2nd radio communication equipment and the 3rd radio communication equipment which is communicating on said notice security level.

[Claim 18]

The radio communications system of claim 6 which is the 3rd radio communication equipment belonging to said radio group, and is characterized by providing further said 2nd radio communication equipment and the 3rd radio communication equipment

which is communicating on the security level which is not lower than said criteria security level.

[Claim 19]

One of said the 1st and 3rd radio communication equipments is the radio communications system of claim 6 characterized by being equivalent to an access point.

[Claim 20]

One of said the 1st and 3rd radio communication equipments is the radio communications system of claim 6 characterized by being equivalent to a wireless terminal.

[Claim 21]

One of said the 2nd and 3rd radio communication equipments is the radio communications system of claim 6 characterized by being equivalent to a wireless terminal.

[Claim 22]

The 3rd radio communication equipment which is the 3rd radio communication equipment besides said radio group, and is communicating with said 2nd radio communication equipment on said notice security level,

The radio communications system of claim 6 which is the 4th radio communication equipment belonging to said radio group, and is characterized by providing further said 2nd radio communication equipment and the 4th radio communication equipment which is communicating on the security level which is not lower than said criteria security level.

[Claim 23]

It is the radio communications system of claim 6 characterized by having the field where said 1st radio communication equipment notified the beacon frame to the 2nd radio communication equipment, transmission of said 1st transmitting frame was required, said beacon frame was supported with said 1st radio communication equipment, and the security frame which is not lower than said criteria security level was indicated.

[Claim 24]

Said 2nd radio communication equipment is the 2nd memory section which memorizes the 2nd security level containing said notice security level,

It reaches with the 2nd frame generating section which determines one security level for said 2nd security level as said notice security level as compared with said criteria security level, and generates said 1st transmitting frame.

It reaches.

The transmitting section which turns this 1st transmitting frame to the 1st radio communication equipment, and transmits,

Furthermore, the radio communications system of claim 6 characterized by providing.

[Claim 25]
The 1st transmitting frame which has the 1st field where notice security level was described is received from the outside of a communication link group,
It is selected from the security level depending on the encryption approach including un-enciphering, and the strength of encryption, and the criteria security level assigned to said radio group is memorized,
The 2nd transmitting frame which has the 2nd field where the connection refusal or connection authorization determined and determined is indicated [authorization / a connection refusal with the radio communication equipment besides said radio group or / connection] in said notice security level as compared with said criteria security level is generated, and it reaches.
The radio approach characterized by turning this 2nd transmitting frame to the radio communication equipment besides said radio group, and transmitting.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]
This invention relates to the radio approach at a radio communications system and a radio-communication-equipment list, and relates to the radio communications system which consists of two or more wireless terminal units and access points especially.
[0002]
[Description of the Prior Art]
As wireless LAN, the wireless LAN system based on IEEE802.11 (an IEEE802.11 system shall contain an IEEE802.11a system, an IEEE802.11b system, etc.) is known for nonpatent literature 1. In this wireless LAN system, a method called WEP (Wired Equivalent Privacy) which can secure privacy like a cable as a cipher system is applied. Therefore, there is non-WEP mode in which the WEP mode in which WEP is applied, and WEP are not applied in the security level of the wireless LAN based on IEEE802.11.
[0003]
In the product of the wireless LAN according to actual IEEE802.11, the communication link by or [any in the WEP mode in which a cipher system called WEP is applied, and the non-WEP mode which is not adapted] is possible, and there is encryption mode which are 64 bits from which the level of encryption differs, and 128 bits in the WEP mode in_which WEP is applied, either is applied to each communication link or each connection link in wireless LAN, and a communication link is realized. Here; the more the level of encryption is high, security level is high and, the more it means being

enciphered more strongly.

[0004]

There is a configuration unit of BSS (Basic Service Set) which consists of two or more wireless clients (it is also hereafter called a terminal.) connected to one set (it is also hereafter called a base station.) of an access point and this access point as one gestalt of the wireless LAN according to IEEE802.11, and there is a system by which two or more BSS is prepared and a network is built.

[0005]

The structural element which connects between this BSS is called DS (Distribution System). A base station, i.e., an access point, has a function linked to this DS, and between BSS and DSs is transmitted to information through an access point. Therefore, a terminal can communicate also with the terminal which belongs to other BSS through an access point.

[0006]

In order to communicate with the terminal which a terminal belongs to BSS and belongs to other BSS through a base station, authentication (authentication) and association (association) procedure are carried out between base stations. Moreover, when a terminal remakes wireless connection in other access points, rear sociation (reassociation) procedure is performed.

[0007]

In the wireless LAN which becomes settled in IEEE802.11, there are a frame for control for an access control (control frame), administrative frames (management frame) including a beacon, and a data frame for data communication (data frame) as a class of frame to exchange. Here, an administrative frame is used for processing of authentication, an association, and rear sociation.

[0008]

When a terminal sends and receives a data frame between access points, authentication and association processing are surely performed before that.

[0009]

In the wireless LAN which becomes settled in IEEE802.11, it asks a base station whether use WEP whose terminal is a cipher system. That is, when WEP can be used, the authentication frame is sent [the base station which required that a terminal should use WEP for a base station, and received this demand] in an authentication demand (authentication request) and received between a base station and a terminal. WEP can be used now based on transmission and reception of such an authentication frame.

[0010]

There is BSS which exists independently of the existing infrastructure as other gestalten of the wireless LAN which becomes settled in IEEE802.11, and this is called IBSS (Independent Basic Service Set). In IBSS, an access point is not prepared but

IBSS is equivalent to the communication configuration with which a terminal communicates each other directly. Moreover, in IBSS, association processing is not performed and, similarly rear sociation processing is not performed. Even if it has not passed through authentication processing between terminals, a data frame can be sent and received in this IBSS.

[0011]

[Nonpatent literature 1] ISO/IEC 8802-11:1999 (E) ANSI/IEEE Std 802.11, 1999 edition

[0012]

[Problem(s) to be Solved by the Invention]

Thus, in the conventional wireless LAN, commo data is enciphered as one of the security countermeasures. The side which received the connection request from the side which emitted the connection request, for example, a terminal, for example, an access point, is required whether to use an encryption function (WEP function) on the occasion of a communication link. In the base station side which received this demand, if use of the WEP function suitable for the demand concerned is possible, the demand concerned would be accepted and the data communication between the terminals concerned will be enciphered. Moreover, it is set leading by the side to which whether it communicates on which security level emitted the connection request.

[0013]

From now on, it will be surmised by wireless LAN that cipher systems which are two or more kinds from which the level of encryption differs, such as a cipher system with security level higher than WEP, are adopted as wireless LAN besides WEP. Therefore, it is required that a setup of fine security level should be attained according to the class of cipher system, encryption level, etc.

[0014]

however, the texture according to the class of cipher system, encryption reinforcement, etc. in the case of about [that it cannot be said that the system which permits only the communication link by the encryption which the minimum encryption level sets beforehand for security reservation, and has the level beyond it for every BSS is made from the conventional wireless LAN], and a communication link -- there is a trouble that warm security level cannot be set up.

[0015]

Furthermore, in IBSS, since it is not necessary to carry out authentication in case a data frame is transmitted, there is a trouble that the data frame which is not enciphered cannot be transmitted and security in a system cannot be secured.

[0016]

Moreover, if the security level beforehand set to the BSS is not securable for every BSS, also in DS communication link which communicates among two or more BSS similarly, there is a trouble that the security level set to each BSS is not securable.

[0017]
This invention is made in view of the situation mentioned above, and that purpose is in providing with the radio approach the radio communications system and radio-communication-equipment list whose radio secure the minimum security level by the encryption beforehand defined into the communication link group, and is possible.
[0018]
[Means for Solving the Problem]
According to this invention
With the receive section which receives the 1st transmitting frame which has the 1st field where notice security level was described from the radio communication equipment besides a communication link group
The memory section which memorizes the criteria security level which was selected from the security level depending on the encryption approach including un-enciphering, and the strength of encryption, and was assigned to said radio group,
It reaches with the frame generating section which generates the 2nd transmitting frame which has the 2nd field where the connection refusal or connection authorization determined and determined is indicated [authorization / a connection refusal with the radio communication equipment besides said radio group, or / connection] in said notice security level as compared with said criteria security level.
The transmitting section which turns this 2nd transmitting frame to the radio communication equipment besides said radio group, and transmits,
The radio communication equipment belonging to said radio group characterized by providing is offered.
[0019]-
Moreover, according to this invention, it is,
It sets to the radio communications system which consists of the 1st radio communication equipment belonging to a radio group, and the 2nd radio communication equipment besides this radio group, and is said 1st radio communication equipment,
With the receive section which receives the 1st transmitting frame which has the 1st field where notice security level was described from said 2nd radio communication equipment
The 1st memory section which memorizes the criteria security level which was selected from the security level depending on the encryption approach including un-enciphering, and the strength of encryption, and was assigned to said radio group,
It reaches with the 1st frame generating section which generates the 2nd transmitting frame which has the 2nd field where the connection refusal or connection authorization determined and determined is indicated [authorization / a connection refusal with said 2nd radio communication equipment, or / connection] in said notice

security level as compared with said criteria security level.
The transmitting section which turns this 2nd transmitting frame to said 2nd radio communication equipment, and transmits,
The radio communications system characterized by providing is offered.
[0020]
Furthermore, according to this invention, it is,
The 1st transmitting frame which has the 1st field where notice security level was described is received from the outside of a communication link group,
It is selected from the security level depending on the encryption approach including un-enciphering, and the strength of encryption, and the criteria security level assigned to said radio group is memorized,
The 2nd transmitting frame which has the 2nd field where the connection refusal or connection authorization determined and determined is indicated [authorization / a connection refusal with the radio communication equipment besides said radio group or / connection] in said notice security level as compared with said criteria security level is generated, and it reaches.
The radio approach characterized by turning this 2nd transmitting frame to the radio communication equipment besides said radio group, and transmitting is offered.
[0021]
[Embodiment of the Invention]
Hereafter, with reference to a drawing, the operation gestalt concerning the radio communications system of this invention is explained.
[0022]
First, in the wireless LAN system in the following operation gestalten, two or more kinds of cipher systems can be applied, the class of the cipher system is distinguished, and, moreover, the security level which ranked and carried out encryption level is defined beforehand. Supposing there is level which is different in each of two or more kinds of cipher systems, for every encryption level in the kind of a certain kind of cipher system, a rank will be attached according to extent of encryption reinforcement, and one security level will be set up to each. Therefore, if the classes of cipher system differ even if it has the same encryption reinforcement, different level as the security level will be given. For example, it considers as enc.0, enc.1, enc.2, --, the thing that has n pieces like enc. (n-1) as security level at order from what has the low reinforcement of encryption. Even if there are two or more kinds of cipher systems of the same reinforcement, the security level from which a rank differs for every class of the shall be set up. Thus, the cipher system of one class corresponds, and even if it is in the cipher system of the same class, when there is moreover two or more level by difference of encryption reinforcement, the security level corresponding to each of the level is set to one security level.
[0023]

Now, in the wireless LAN system specified to present IEEE802.11, as for the minimum level of security level, encryption nothing, i.e., the level for which WEP (Wired Equivalent Privacy) is not adapted, corresponds.

[0024]

There is two level as WEP is further constituted from 64 bits or 128 bits, even if it is, when WEP is applied to present IEEE802.11 with the wireless LAN product according to a convention. then -- the following -- operation -- a gestalt -- an example -- **** -- plurality -- security -- level -- ****** -- present -- IEE -- 802.11 -- a convention -- following -- wireless LAN -- the same -- (-- one --) -- " -- WEP -- nothing -- " -- (-- two --) -- " -- WEP -- **** -- 64 -- a bit -- WEP -- use -- " -- (-- three --) -- " -- WEP -- **** -- 128 -- a bit -- WEP -- use -- " -- three -- a ** -- level -- it is -- a case -- as an example -- explaining . in this case, the thing with the highest security -- (3)" -- those with WEP -- 128-bit WEP -- use" -- it is -- this -- subsequently -- (4)" -- the security of use" is high about 64-bit WEP with WEP. that is, "" "having no enc.0(1) WEP" -- corresponding -- " -- those with enc.1"(2)" WEP -- 64-bit WEP -- use" -- corresponding -- " --" "shall correspond 128-bit WEP to use" with enc.2(3) WEP

[0025]

In the following explanation, the case of only the cipher system of one class of WEP is explained. However, if two or more level can be set up according to a difference of the class of cipher system, and the strength of security even if it is cipher systems other than WEP, this invention is applicable even if it is in which cipher system like explanation of the following operation gestalten.

[0026]

The operation gestalt of this following invention explains the case where this invention is applied to the wireless LAN system to which it was specified at IEE802.11. Especially the case where it applies to the base station or terminal which constitutes the wireless LAN system to which the radio communication equipment of this invention was specified at IEE802.11 is explained.

[0027]

(1st operation gestalt)

First, the communication system with which the base station AP 1 where wireless connection of two or more terminals (WL11-WL12), for example, two terminals, and this terminal (WL11-WL12) is made as a radio communications system constitutes one BSS (BASIC service set) in the 1st operation gestalt of this invention is explained.

[0028]

Drawing 1 shows typically the 1st BSS (hereafter referred to as BSS1 simply). BSS1 consists of two wireless terminals (it is hereafter called a terminal) WL11 and WL12 at two or more terminals connected to the base station AP 1 and base station AP 1 as an access point, for example, here.

[0029]
In addition, the base station AP 2 belonging to the 2nd BSS (hereafter referred to as BSS2 simply) which is different in 1st BSS1, and the terminal WL13 which has not joined BSS1 and BSS2 are also shown in drawing 1 .
[0030]
The minimum security level (enc_low) permitted there is set to BSS1. In the radio communications system concerning this operation gestalt, the minimum security level (enc_low) permitted by BSS1 supposes that it is security level "enc.1." The purport whose minimum security level (enc_low) to permit is security level "enc.1" is expressed as enc_low=enc.1 to drawing 1 . In the base station AP 1, security level"enc.1 level [security] enc.2" with high level shall also be supported rather than" "besides the security level "enc.1." Therefore, the highest usable security level (enc_high) is set to "enc.2" by BSS1. The purport whose highest security level (enc_high) is "enc.2" is expressed in drawing 1 as enc_high=enc.2. As for the terminal or base station connected to a base station AP 1 and this base station AP 1, it is beforehand set as the base station AP 1 that a communication link is carried out on the security level more than "enc.1." It is beforehand set as the base station AP 1 between the terminal for similarly, relaying this base station AP 1 and communicating to other equipments, or the base station that a communication link is carried out on the security level more than "enc.1."
[0031]
On the other hand, the security level which a terminal WL11 has presupposes that "enc.0", "enc.1", and the security level that a terminal WL12 has are "enc.0", "enc.1", and "enc.2."
[0032]
Drawing 2 shows the block of the circuitry of the base station AP 1 shown in drawing 1 . In addition, in the following explanation, when there is no need of distinguishing a base station AP 1 and a base station AP 2, in the explanation common to both, a base station AP is only called.
[0033]
In drawing 2 , the sending signal from a terminal is received by the antenna 20, and an input signal is generated by processing including a recovery and decode in a receive section 11. In the transmitting section 12, the sending signal which should transmit to a terminal through an antenna 20 is generated, and these sending signals are supplied to an antenna 20.
[0034]
Predetermined reception which the input signal from a receive section 11 was inputted into the reception-control section 13, for example, was based on the IEEE802.11 system (an IEEE802.11 system shall also contain the IEEE802.11 system upon which it will be decided an IEEE802.11a system, an IEEE802.11b system, and

from now on in the following explanation) is carried out. In this reception-control section 13, decryption processing corresponding to each of two or more security level which a base station supports is performed, and an input signal is compound-ized (decrypt) and is changed into compound-ized data. This compound-ized data is supplied to the information processing section 15, and is divided into video, an audio, a text, and the data of other types, and required processing is performed.

[0035]

The transmission-control section 14 carries out predetermined transmitting processing based on IEEE802.11 of generating the data for transmitting to a terminal by broadcasting or the unicast based on the data supplied from the information processing section 15 etc. It has given the data which should transmit the encryption processing corresponding to each of two or more security level which a base station supports in this transmission-control section 14. The data generated in the transmission-control section 14 are transmitted to a terminal as a sending signal through the transmitting section 12. In addition, the security table 21 shown in drawing 2 is explained later.

[0036]

Drawing 3 shows roughly an example of the circuitry of the terminals WL11, WL12, and WL13 shown in drawing 1 with a block. In addition, in the following explanation, when there is no need of distinguishing terminals WL11, WL12, and WL13 etc., in the explanation common to all terminals, it is only called Terminal WL.

[0037]

A terminal WL consists of the information-processing sections 108 and the security tables 110 which display on the display which generated the reception-control section 105 which controls the receive section 101 which receives an input signal through an antenna 100 and an antenna 100, and a receive section 101, the transmitting section 107 which transmits a sending signal through an antenna 100, the transmission-control section 106 which controls this transmitting section 107, and the data transmitted, or received, which carries out data processing for example, which is not illustrated.

[0038]

The information processing section 108 creates transmit data based on the data which received data from the cable network 109 connected to this information processing section 108, or were generated by actuation of a user. This transmit data will pass transmit data to the transmitting section 107 in response to this Request to Send, if transmission of that transmit data is directed by the user and a Request to Send arises. In the transmitting section 107, it is changed into the MAC frame (medium access control frame) which this transmit data is changed into the digital data defined by specification, for example, specifies an IP packet by IEEE802.11, the MAC frame as digital data is changed into predetermined frequency, for example, the

radio signal it is [radio signal] 2.4GHz, and it is sent as an electric wave from an antenna 100.

[0039]

On the other hand, it is changed into the MAC frame as digital data in a receive section 101, received data are extracted from the information field in this MAC frame, and the input signal received with the antenna 100 is sent to the information processing section 108. This information processing section 108 processes displaying received data on a display etc. In addition, the information processing section 108 performs various information processing besides the above. Moreover, the security table 110 is explained later.

[0040]

The MAC frame specified by IEEE802.11 consists of the frame-check-sequence (FCS) fields for investigating whether the MAC header which is a maximum of 30 bytes to which various control information was dedicated, the data field (frame body) in which the data which are a maximum of 2312 bytes are settled, and data were sent correctly, as shown in drawing 4 . The frame control field where the information which controls the MAC frame is stored, and Duration/IDfield ID of the terminal with which a terminal can send data, and which is called Association ID in a standby time (duration) or IEEE802.11 until it becomes like like is described to be are contained in the MAC header. If BSS is equipped with the base station AP, the MAC Address of a base station AP will be described as ID of this BSS. Moreover, the field and the sequential control field of the address 4 are prepared for the MAC header from the field of the address 1. When transmitted to other access points from an access point with a data frame, the addresses 1-4 are assigned as follows. That is, the MAC Address of the final destination in communication system (Destination Address) is described, the MAC Address of the transmitting origin in communication system (Source Address) is described by the field of the address 1, the MAC Address of the transmission place which sends the MAC frame concerned to the field of the address 3 directly is described, and the MAC Address of the transmitting origin which sends the MAC frame concerned to the field of the address 4 directly is described by the field of the address 2 in it.

[0041]

The protocol version field where the version of a protocol is described is established in frame control of the MAC frame, and the type field and the subtype field are established in it following this. There are the following three types of the MAC frames, and this type is described by the type field (2 bits) in frame control. Moreover, the type of subtype is further shown in a detail in the subtype field (4 bits). That is, it is (1) as a type. There are a frame for control for an administrative frame and (2) access controls and a data frame for (3) data communication. (1) There are a beacon (Beacon), a frame of authentication (Authentication), a frame of an association

(Association), an association request frame, an association response frame, etc. in an administrative frame as a subtype. Moreover, (2) There are frames for control, such as ACK (Acknowledgment), RTS (Return To Send), and CTS (Clear To Send), among the frames for control as a subtype. The subtype in the MAC frame of the above specific classes is further shown in the detail in the subtype field (4 bits).

[0042]

In addition, the To DS field (1 bit) and the From DS field (1 bit) are included in frame control. These are used when the MAC frame is a data frame, and with the frame of the frame of the other class, for example, authentication, and an association, "0" is always written in and they are not used. If the destination of data is Cable LAN, an access point, or DS when the MAC frame is a data frame, the bit of 1 will be described by this To DS field, and the bit of 1 will be described by this From DS field if the transmitting origin of data is Cable LAN, an access point, or DS. And also [like the reserve field (reserved field), the WEP field, and the order field (order field)], the field is further prepared for frame control. Information can be written in the reserve field which does not especially still have a law by the user. As shown in drawing 4 , according to either the type of a frame and the subtype or the type of a frame and the subtype, some fields are considered as reserve. With the operation gestalt of this invention, encryption level may be described by this reserve field so that it may explain later. This encryption level is defined according to the attribute of transmit data. If it is contents data with which confidentiality is demanded, high encryption level will be defined and that encryption level will be described by this reserve field. The encryption level of this reserve field may be used in case [of / between an access point and a terminal] a handshake is carried out. The bit of 1 is set to the WEP field when WEP is used.

[0043]

With reference to drawing 1 , BSS1 is explained again.

[0044]

In BSS1 shown in drawing 1 , it is defined beforehand that a communication link is performed on the minimum security level (here "enc.1") beforehand set to this BSS1. That is, a communication link on the security level more than "enc.1" is performed within the limits of the security level on which security level "enc.1" or a base station AP 1 is supporting the base station AP 1 which constitutes BSS1, and each of terminals WL11-WL12.

[0045]

Each of a base station AP 1 and terminals WL11-WL12 is equipped with the storage section, and the security table is prepared in this storage section. As for the security level which each of any the security level which base station AP1 self supports, and the security level of the minimum level [in / in the inside of this security level / BSS1] are, and terminals WL11-WL12 is supporting, it is memorized by the security

table of a base station AP 1 what kind of thing it is. Moreover, it is desirable information required for encryption and a decryption of each security level, and it is desirable that the seed information for generating a cryptographic key or a cryptographic key etc. is memorized by this security table (information required for such encryption and a decryption is only called a code parameter here.). Moreover, each of terminals WL11-WL12 is also equipped with the storage section the security table is remembered to be, and the security level of the minimum level in the security level which BSS1 supports, the security level which is supporting other terminals, the code parameter further corresponding to each security level, etc. are memorized by the security table.

[0046]

As shown in drawing 5 , it registers with the security table 21 of a base station AP 1 beforehand with the code parameter which is data which need for the code and compound of each security level the security level supported in BSS1 to which the base station AP 1 concerned belongs and the security level which all the terminals WL11-WL12 belonging to BSS1 have. Moreover, the security level set up as security level of the minimum level in BSS1 to which a base station AP 1 belongs is registered into this security table 21 so that it may be identifiable. In drawing 5 , the security level "O" mark which means the minimum level to "enc.1" is recorded.

[0047]

The private key (key1, key2) with which the encryption parameter is specified by IEEE802.11 as an example in WEP, IV (Initialization Vector), etc. are assumed. In addition, in the following explanation, security level and the code parameter corresponding to this security level may be called security information.

[0048]

Drawing 6 shows the contents of registration of the security table 110 of the terminals WL11-WL12 in BSS1. As shown in drawing 6 , the security information which each terminal in BSS1 and a base station AP 1 have is beforehand registered into the security table by the side of a terminal. As security information corresponding to a base station AP 1, as shown in drawing 6 , only the security information of the minimum level beforehand set as BSS1 to which this base station AP 1 belongs may be registered. Moreover, the security table 110 by the side of a terminal may completely be the same as the security table 21 by the side of the base station shown in drawing 5 .

[0049]

Moreover, the base station AP 1 registered into the security table shown in drawing 5 and drawing 6 and the security level of each terminal should just be the things more than the minimum level beforehand defined by BSS1. Furthermore, about the security information corresponding to each terminal, only the security level used in BSS1 in the case of an actual communication link may be registered. That is, when each

terminal is directly linked to an access point and it is directly linked to the security information about an access point, or a terminal, it is the security information about a terminal and each terminal can be held on the security table about the security information currently supported with the terminal in BSS.

[0050]

Moreover, the security table shown in drawing 5 and drawing 6 is set up at the time of initialization of BSS1. The table of the format shown in drawing 5 and drawing 6 is displayed as a setting screen, and you may make it input a setting matter on this screen at the time of initialization. In the table shown in drawing 5 and drawing 6 , AP1, WL1, and WL2 are specified by the MAC Address of a base station AP 1 and terminals WL1 and WL2, respectively.

[0051]

In addition, any [the security table shown in drawing 5 and drawing 6] information in the case of initialization does not need to be written in, either. However, security information can be written in, if it is linked in the mode in which it does not encipher so that an access point AP 1 and terminals WL1 and WL2 may explain later with reference to drawing 7 . Namely, an access point AP 1 and terminals WL1 and WL2 acquire the security information about an access point AP 1 and terminals WL1 and WL2, and write in each security table, BSS1 is established after that with an access point AP 1 and terminals WL1 and WL2, and the minimum security level within BSS1 should just be set up.

[0052]

By BSS1 shown in drawing 1 , a communication link is performed between a base station AP 1 and terminals WL [WL11-] 12 on the security level more than minimum security level "enc.1" beforehand set up to this BSS1.

[0053]

Next, the case where the terminal WL13 which has not joined the base station AP 1 of BSS1 shown in drawing 1 at this BSS1 is connected is explained with reference to the flow chart shown in drawing 7 .

[0054]

A terminal WL13 receives the beacon (Beacon) frame specified to IEEE802.11 transmitted from a base station AP 1. according to a convention of IEEE802.11 -- reception of a beacon frame -- then -- next, although authentication (authentication) and an association (association) protocol continue, the security level of a terminal WL13 is written in into the frame for this authentication or an association as information notified to a base station AP 1.

[0055]

The procedure in the case of notifying the security level of a terminal WL13 to a base station AP 1 with the frame of authentication as an example is shown in drawing 7 . In this procedure, it is assumed that the security level which a terminal WL13 has is

"enc.0" and "enc.1."

[0056]

Drawing 8 (a) shows the format of the frame body in the frame of the authentication as a MAC frame shown in drawing 4 specified to IEEE802.11. The authentication algorithm which distinguishes the common encryption keying system which uses for an authentication frame the open system which does not use a common cryptographic key, and a common cryptographic key is described. "0" is described with an open system by the authentication algorithm number, and "1" is described with a common encryption keying system. In the open system specified by the authentication algorithm number 0, as shown in drawing 8 (b), the frame of ATSN(Authentication Transaction Sequence Number) =1 and =2 is prepared as a demand frame of authentication. The frame of the authentication of ATSN=1 is sent to a base station AP 1 from Terminal WL, and the status code field (Status Code field) is considered as reserve. The frame of the authentication of ATSN=2 is sent to Terminal WL from a base station AP 1, and the code of a connection refusal or connection authorization is indicated by the status code (Status Code) as the status. In the open system specified by the authentication algorithm number 0, the challenge text in which the frame of authentication is enciphered is not prepared. In the common encryption keying system, the frame of ATSN(Authentication Transaction Sequence Number) =1-4 is prepared as a demand frame (authentication request) of authentication. The frame of the authentication of ATSN=1 and ATSN=3 is sent to a base station AP 1 from Terminal WL, and the status code is considered as reserve. The frame of the authentication of ATSN=2 and ATSN=4 is sent to Terminal WL from a base station AP 1, and the code of a connection refusal or connection authorization is indicated by the status-code as the status. a common encryption system -- ATSN= -- the challenge text for encryption is prepared for the frame of the authentication of 2 and 3, and the frame of the authentication of ATSN=3 is enciphered. on the other hand, ATSN= -- the challenge text for encryption is not prepared for the frame of the authentication of 1 and 4.

[0057]

The frame of the authentication specified by ATSN=1 is transmitted from the side which emits a connection request. With this demand frame, that status code field is considered as reserve, and is intact now. Therefore, security level "enc.1" of the side which emits a connection request, or "enc.2" can be written in this status code field. In explanation of the following operation gestalten, security level "enc.1" of the side which emits a connection request, or "enc.2" shall be written in Statuscode field. The data in which security level (for example, "enc.1") to use for the frame of this authentication of ATSN=1 by the communication link with a base station AP 1 in the transmitting section 107 of a terminal WL13 is shown are written in the term of that status code, and as the frame of this authentication of ATSN=1 shows step S2 of

drawing 7 , it is transmitted to a base station AP 1. In addition, this security level may be written in the reserve field of either of the MAC frames shown in drawing 4 .

[0058]

Processing actuation of the base station AP 1 which received the frame of the authentication of ATSN=1 is explained. It is detected by the terminal WL13 as are already indicated, and the beacon frame always emitted from the base station AP 1 shows step S1. After this detection, the transmission-control section 106 of a terminal WL13 prepares the authentication frame of ATSN=1, and writes security level "enc.1" or "enc.2" in the predetermined part of that frame, for example, the status code in the frame body, with reference to the security table 110. The authentication frame in which security level was written is specified as the address 2 by making into the destination the base station AP 1 corresponding to the beacon frame detected by the transmission-control section 106 of a terminal WL13, and as shown in step S2, it is transmitted to a base station AP 1. a base station -- AP -- one -- authentication -- a frame -- receiving -- a base station -- AP -- one -- a reception control -- the section -- 13 -- having received -- ATSN -- = -- one -- authentication -- a frame -- predetermined -- a part -- for example, -- a frame -- the body -- inside -- a status code -- writing in -- having -- **** -- a terminal -- WL -- 13 -- security -- level -- " -- enc . -- one -- " -- or -- " -- enc . -- two -- " -- taking out -- a base station -- AP -- one -- security -- a table -- 21 -- registering -- having -- **** -- BSS -- one -- the minimum -- level -- security -- level -- "enc_low" -- comparing . a step -- S -- three -- being shown -- as -- a terminal -- WL -- 13 -- from -- notifying -- having had -- this -- a terminal -- WL -- 13 -- security -- level -- " -- enc . -- one -- " -- or -- " -- enc . -- two -- " -- a base station -- AP -- one -- supporting -- **** -- security -- level -- " -- enc . -- one -- " -- or -- " -- enc . -- two -- " -- it is -- moreover -- BSS -- one -- inside -- it can set -- the minimum -- level -- security -- level -- "enc_low" -- more than -- the time -- **** -- a terminal -- WL -- 13 -- connection -- granting a permission -- ** -- judging . Although it is the security level which the base station AP 1 is supporting when the security level of a terminal WL13 is not the security level which the base station AP 1 is supporting or, it is judged that connection of a terminal WL13 is refused at the time under of the security level of minimum level "enc_low" in BSS1.

[0059]

In step S3, when a base station AP 1 refuses connection of a terminal WL13, the authentication frame of ATSN=2 is prepared for IEEE802.11 by the transmission-control section 12 according to a convention, the code of the purport whose connection is failure is written in the status code, and as shown in step S4, the authentication frame of ATSN=2 is answered by the terminal WL13. Reception of the authentication frame of ATSN=2 to which description which refuses connection as a terminal WL13 is shown in step S5 was carried out judges whether it is eye N time.

This N time is equivalent to the number of the security level currently written in the security table 110 by the side of a terminal (=N individual). At the beginning, as level with the low security level which the base station AP 1 is supporting, a terminal WL13 notifies the security level of this low level to a base station, and if refused, that security level will be raised, and the security level raised as shown in step S2 is notified. The security level of N individual which the security table 110 by the side of a terminal is supporting is notified, and as shown in step S5, when N time is covered and a terminal WL13 receives the authentication frame of ATSN=2, it judges that it was refused by connection from a base station AP 1, and connection procedure is interrupted as shown in step S15 in this phase.

[0060]

On the other hand, when permitting connection of a terminal WL13 A base station AP 1 that the code parameter corresponding to the security level notified from the terminal WL13 should be shared with a terminal WL13 The authentication frame of ATSN=2 which transmit the Chillan range text to IEEE802.11 according to a convention as shown in step S6 is prepared. The code of the purport whose reception of the authentication frame of ATSN=1 is a success is written in the status code of this authentication frame, and as shown in step S6, a terminal WL13 is answered.

[0061]

At a terminal WL13, reception of the authentication frame of ATSN=2 decides the security level between a base station AP 1 and a terminal WL13, for example, security level"enc.1." Moreover, a terminal WL13 is enciphered using the WEP function in which a terminal WL13 has the frame body which contains a challenge text etc. as a code parameter corresponding to security level according to a convention of IEEE802.11 using IV and the private key which were acquired beforehand by the user as shown in step S7. Furthermore, a terminal WL13 prepares the authentication frame of ATSN=3, and copies a challenge text to the frame body from the authentication frame of ATSN=2. This terminal WL13 is transmitted to a base station AP 1, as a frame is enciphered and it is shown in step S8.

[0062]

In the base station AP 1 which received the authentication frame of ATSN=3, the encryption challenge text stored by decoding the authentication frame of ATSN=3 received as shown in step S9 with the private key which the base station AP 1 currently similarly shared between the terminal WL13 by IEEE802.11 according to the convention has will be taken out. This compound-ized challenge text is compared with the transmitted challenge text, and as shown in step S10, encryption / compound-ization is verified based on that comparison result.

[0063]

If a verification result is "failure", the authentication frame of ATSN=4 which similarly notify that to IEEE802.11 according to a convention will be prepared, the code of the

purport whose verification result is "failure" will be written in the status code, and as shown in step S11, the authentication frame of ATSN=4 will be answered by the terminal WL13. "Failure" of a verification result means that the cipher system is different with the base station AP 1 and the terminal WL13. Therefore, as shown in step S14, it is checked that the authentication frame of ATSN=4 is less than M times, the cipher system in a terminal WL13 is changed, and it is returned to step S2, and step S10 is repeated from step S2. Here, it can respond to the number of the cipher system which the terminal WL13 is preparing M times, and, as for a terminal WL13, the authentication frame of M time ATSN=4 can be received. thus, even if the terminal WL13 received the authentication frame of M time ATSN=4, when a cipher system was not in agreement, as for the terminal WL13, connection with a base station AP 1 was refused -- it is judged. Therefore, in a terminal side, as shown in step S15, connection procedure is ended, noting that the cipher system which a base station AP 1 offers is not prepared.

[0064]

On the other hand, if the verification result in step S10 is "a success", a base station AP 1 will transmit the authentication frame of ATSN=4 which similarly notify that to IEEE802.11 according to a convention as shown in step S12 to a terminal WL13. At a terminal WL13, reception of this frame starts the association specified to IEEE802.11 which is the following procedure as shown in step S12. That is, a terminal WL13 answers delivery and this request in an association request frame as shown in step S13 in a base station AP 1, and processing actuation which followed the convention at IEEE802.11 which returns a base station AP 1 to the association response terminal WL13 is performed. After an association is completed normally, a data frame is transmitted and received between a terminal WL13 and a base station AP 1. The data frame transmitted and received is enciphered by the 64-bit WEP function equivalent to the encryption beforehand defined by the above-mentioned procedure, for example, the security level of "enc.1=enc.low."

[0065]

In addition, in a terminal WL13 and a base station AP 1, when the security level and the code parameter of the communication link between the terminal WL13 and a base station AP 1 are decided, mutual security information is registered into the security table 21,110. That is, at a terminal WL13, after acquiring a code parameter at step S7 shown in drawing 7 , the security information of a base station AP 1 is registered into the security table 110. Moreover, in a base station AP 1, after verification is successful at step S10 of drawing 7 , the security information of a terminal WL13 is registered into the security table 21. That is, security information is registered into the security table 21 of an access point AP 1 by relation with this address by choosing the suitable address field which shows the address of the terminal WL13 in the MAC frame shown in drawing 4 . As shown in drawing 10 , the security information whose

"connection place" is a terminal WL13 is newly registered into the security table of a base station AP 1. The security information whose "connection place" is a base station AP 1 similarly is newly registered also into the security table of a terminal WL13. That is, security information is registered into the security table 110 of a terminal WL13 by relation with this address by choosing the suitable address field which shows the address 1 of the base station AP 1 in the MAC frame shown in drawing 4 . The security level of the security information in this newly added terminal WL13 is equivalent to the security level which the terminal WL13 has required at step S2 of drawing 7 .

[0066]

Moreover, if the security information of a base station is registered into the security table by the side of a terminal, a terminal can choose beforehand the security level more than the minimum level of the base station, consequently will be step S3, and will not have connection refused from the base station concerned. Here, the security information of a base station has the security level more than the minimum level beforehand set to BSS to which the base station concerned belongs at least. What is necessary is just to notify this security level to a base station, as the security level more than the minimum level set to the base station in the base station out of the security level which the terminal itself is supporting is chosen and it is shown in step S2 in drawing 7 in case a terminal will re-connect with a base station, if it puts in another way.

[0067]

Moreover, it is desirable that the security information of the security level more than minimum level enc_low beforehand set to BSS to which the base station concerned belongs to the security table of a base station AP at least as security information about Terminal WL is registered. In this registration, about BSS to which a base station belongs, BSS is specified in the address indicated by the suitable address field in the MAC frame shown in drawing 4 , and this address and security level are described by the security table. If there is registration about such BSS, the security level on which it is more than the minimum level concerned, and the terminal concerned can moreover support the security level used for the unicast communication link to the terminal concerned from a base station will be chosen beforehand, and the thing of it can be carried out. Moreover, the security level in the multicast communication link to the terminal WL in BSS to which a base station AP belongs, and a broadcasting communication link is also more than the minimum level enc_low concerned, and can choose beforehand the thing of the security level currently moreover supported at all the terminals that should receive it. That is, as shown in step S5 of drawing 7 , when connection is refused from a base station AP 1, different security level of desirable more high level from the security level notified previously is notified, and what connection requires again is made. The connection

request only of the count M of maximum predetermined becomes possible, notifying one [at a time] the security level which a terminal WL13 has.

[0068]

You may make it a base station AP 1 notify all the security level more than security level enc_low of the minimum level beforehand set as BSS1, or minimum level enc_low which the base station AP 1 is supporting to the terminal WL13 of connection-request origin. You may make it notify this notice using current a non-used frame among the administrative frame of the MAC frame specified to IEEE802.11, and the frame for control. For example, a subtype corresponds with an administrative frame and frames, such as "0000" - "1001", correspond [a subtype] with frames, such as "0110" - "0111", and the frame for control. When a base station AP 1 refuses connection of a terminal, after transmitting the authentication frame of ATSN=2, this intact frame is transmitted and you may make it notify all the security level more than minimum level enc_low to a terminal WL13 in step S4 shown in drawing 7 . Moreover, step S4 or a frame intact before setting step S6 and transmitting the authentication frame of ATSN=2 may be transmitted, and all the security level more than minimum level enc_low may be notified to a terminal WL13. Furthermore, during processing of authentication or an association, before transmission and reception of a data frame begin, the suitable time is chosen at its own discretion, and an access point AP 1 transmits an intact frame, and you may make it notify all the security level more than minimum level enc_low to a terminal WL13.

[0069]

As shown in the frame of the association of the MAC frame specified to IEEE802.11 at drawing 9 (a), drawing 9 (b), and drawing 9 (c), the reserve field is prepared as a free space in "the KYAPA kinky thread tea information (Capability information)" on the frame body. You may make it a base station AP 1 notify all the security level more than security level enc_low of the minimum level of BSS1, or the minimum level enc_low concerned which the base station AP 1 is supporting to the terminal WL13 of connection-request origin at a terminal WL13 using this free space.

[0070]

thus, the case where the terminal WL11 which belongs to a base station AP 1 in BSS1, and the terminal WL13 which does not belong in BSS1 other than WI12 tend to connect with the operation gestalt of the above 1st -- first

(1) This terminal WL13 notifies the security level of terminal WL13 self to a base station AP 1. In the flow shown in drawing 7 , this notice uses the frame of authentication.

[0071]

(2) In a base station AP 1, the security level notified from this terminal WL13 is the security level currently supported in the base station AP 1, and moreover, when it is more than the security level of minimum level enc_low beforehand set to BSS1, permit

connection of a terminal WL13 and continue processing actuation for connection. However, when the security level notified from a terminal WL13 does not fulfill the security level of the minimum level beforehand set to BSS1, connection of a terminal WL13 is refused.

[0072]

(3) When permitting the connection from a terminal WL13, recognition processing for sharing, the information, i.e., the code parameter, for encryption and a decryption, is performed if needed.

[0073]

Thus, according to the operation gestalt of the above 1st, radio which secured minimum security level by the encryption beforehand defined into each group for every basic group of wireless LAN called BSS is realized.

[0074]

Preferably, if the security level of record level enc_high is notified by the base station AP 1 among the security level on which terminal WL13 self supports a terminal WL13 in the above (1), the opportunity for a base station AP 1 to refuse connection of a terminal WL13 will decrease. Moreover, if the security level of record level enc_high is notified to a base station AP 1, by 1 time of the connection request, the propriety of connection with the base station AP 1 concerned can be judged, and useless traffic can be reduced as a result.

[0075] Moreover, as for the base station or each terminal in BSS1, it is desirable to register into a security table the security information of the security level more than minimum level enc_low beforehand set to BSS1 used in case it communicates with the base station in BSS1 or a terminal, respectively. A base station or each terminal can choose beforehand the minimum security level which is not denied connection as security level notified in case a connection request is carried out to the desired terminal and desired base station which are pinpointed in the address with reference to this security table.

[0076]

Although only one security level which expects that a terminal WL13 uses by the communication link with a base station AP 1 in step S2 is notified to the base station AP 1 with the operation gestalt of the above 1st, it is clear that it is not what is restricted in this case. Even if it is not all that terminal WL13 self has, or all, two or more security level may be notified to a base station AP 1 from a terminal WL13. Moreover, only security level enc_high of a record level may be notified to a base station AP 1 from a terminal WL13 among the security level which a terminal WL13 supports.

[0077]

In step S2, the processing actuation of the base station AP 1 in the case of notifying two or more security level, even if it is not all altogether which terminal WL13 self has

is explained.

[0078]

In step S2 shown in drawing 7 , two or more security level which terminal WL13 self has is transmitted to a base station. It judges whether the security level which is the security level more than security level enc_low equivalent to the minimum level [in / in this security level in a base station AP 1, and / at step S3 / BSS1], and self-equipment is moreover supporting is contained. It is judged that a base station AP 1 permits connection of a terminal WL13 when the security level currently supported is contained. Moreover, it is judged that a base station AP 1 refuses connection of a terminal WL13 when the security level currently supported is not contained. When refusing connection of a terminal WL13, it progresses to step S4. When permitting connection of a terminal WL13, both the base stations AP 1 choose the security level more than minimum level enc_low in BSS1 next among the security level which the terminal WL13 and the base station AP 1 are supporting. A base station AP 1 chooses one of them, when two or more security level more than minimum level enc_low in BSS1 exists. What is necessary is just to choose one of them, even if it is those any although there are the minimum thing or the highest thing, and other various selection criteria in it about this selection. A base station AP 1 makes one selected security level the security level used for the communication link between terminals WL13. For example, supposing the security level notified from the terminal WL13 is "enc.0" and "enc.1", the connection with the base station AP 1 of a terminal WL13 will be permitted, and the security level of the communication link between a terminal WL13 and a base station AP 1 will be chosen with "enc.1."

[0079]

When this selected security level needs to be notified to a terminal WL13, before transmitting the authentication frame of ATSN=2 at step S6 of drawing 7 , an intact frame etc. may be used now among the administrative frame of the MAC frame specified to above-mentioned IEEE802.11, and the frame for control.

[0080]

At a terminal WL13, subsequent processing can be prepared in response to the notice of the selected security level.

[0081]

Within BSS1, if it is the security level more than minimum level enc_low beforehand set to BSS1, it is not necessary to necessarily communicate on the same security level.

[0082]

Moreover, you may make it communicate on different security level according to a connection partner within BSS1. That is, if a base station AP 1 is the security level more than minimum level enc_low beforehand set to BSS1, especially limitation will not have it about communicating with which terminal on which security level here. The

secrecy nature of radio can be improved by communicating on the security level from which a base station AP 1 differs for every terminal.

[0083]

Although drawing 7 was explained as actuation at the time of connection between the terminals WL13 and base stations AP 1 which have not joined BSS1, it may transpose the terminal WL13 of the above-mentioned explanation to each of terminals WL11-WL12 which has joined BSS1. If the procedure shown in drawing 7 is followed, respectively also when [of terminals WL11-WL12] it is going to connect with a base station AP 1, security level different each time can be notified at step S2 of drawing 7 , and the security level according to the purpose can be changed at every connection. In this case, since the security level of the minimum level of BSS1 is registered into the security table of each terminal, the security level more than this minimum level is chosen among the security level which each terminal supports, and it is notified at step S2. Moreover, even if it does not change security level, code parameters (in the case a private key, IV, etc. of WEP) can also be changed in the case of subsequent authentication.

[0084]

Similarly, the procedure in the case of the connection request from the terminal of explanation of drawing 7 to a base station is applicable to a base station also as a procedure in the case of a connection request from the base station belonging to mutually different BSS. That is, it can transpose to the base station AP 2 of BSS2 in the base station belonging to other BSS which is [terminal / WL13 / of explanation of drawing 7] different in a base station AP 1, and is [base station / AP 2] different in BSS1, for example, here. Thus, according to the 1st operation gestalt, also in the communication link, i.e., DS communication link, between base stations, a communication link is realized above each minimum security level.

[0085]

In case it communicates with the terminal WL12 in BSS1, for example, other terminals in BSS1 with the same terminal WL11, for example, a terminal, you may connect and communicate to a base station AP 1 through a base station AP 1, and direct communication may surely be carried out between terminals without a base station AP 1.

[0086]

When it is going to connect with terminals WL11-WL12 and the partner by whom the base station AP 1 is registered into each security table, the authentication for transmitting and receiving security level and a code parameter etc. may be omitted. What is necessary is just to communicate a requiring agency with reference to the security table at the side which received the connection request, on the security level more than the minimum level beforehand defined within BSS1, if the transmitting origin of the frame is registered into the own security table.

[0087]

Only the security information of the security level used by the communication link in the meantime in the past may be registered into a base station AP 1 and each security table of terminals WL11-WL12 for every connection partner. This security information registered is equivalent to the security level more than minimum level enc_low in BSS1.

[0088]

The security level set as the security information and BSS1 of all security level which the each supports as the minimum level may be registered to each equipment which constitutes BSS1 as, as for all of the base station AP 1 in BSS1, and the security table of terminals WL11-WL12, the same contents indicated and shown at drawing 5 at the time of initialization.

[0089]

Moreover, within BSS1, "enc.1" which is the minimum security level which also permits a base station AP 1 and terminals 11-WL 12 by BSS1 supports. Therefore, either of the terminals WL11-WL12 shall be enciphered in a data frame etc. on the minimum security level which permits the frame body of the frame within BSS1 when broadcasting, a multicast and. Thereby, as BSS1, the minimum security level to permit is securable.

[0090]

Moreover, with the operation gestalt of the above 1st, the recognition processing for sharing a code parameter between the connection-request point with the check of the security level which is supporting connection-request origin connection-request origin is summarized at the time of the authentication to which it is specified at IEEE802.11, and is performed. However, these two processings can be divided and processing can also be performed at the time of the association to which the former is specified at IEEE802.11. Moreover, also when performing an association previously, next performing authentication, it thinks. In this case, two above-mentioned processings may be summarized at the time of authentication, and may be performed, and it may be made to carry out by dividing at the time of an association and authentication. However, when dividing two above-mentioned processings, the direction which performed the check of security level in advance of the recognition processing for sharing a code parameter preferably is desirable when securing security.

[0091]

(2nd operation gestalt)

The communication system concerning the 2nd operation whose base station of BSS1 as minimum security level shown in drawing 1 defined beforehand in broadcasts the minimum security level defined by BSS1 concerned is explained. In this explanation, in the communication system concerning the 2nd operation gestalt, it omits and that

different point is explained with reference to drawing 12 about the same explanation as the 1st operation gestalt.

[0092]

In the communication system concerning the 2nd operation gestalt, the minimum security level of the BSS concerned is written in the beacon frame specified to IEEE802.11, and this beacon frame is transmitted.

Drawing 11 shows the format of the frame body of the beacon frame which has the structure of the MAC frame specified to IEEE802.11. In "the KYAPA kinky thread tea information (Capability information)" on this beacon frame, the reserve field is prepared as a free space. Even if a base station AP 1 is not all the security level or all more than the security level of the minimum level of BSS1, or the minimum level concerned which the base station AP 1 is supporting, it writes two or more security level in this reserve field, and notifies that security level to Terminal WL.

[0093]

On a beacon frame, even if the transmission-control section 14 of a base station AP 1 is not all the security level or all more than the security level of the minimum level of BSS1, or the minimum level concerned which the base station AP 1 is supporting, it writes in and broadcasts two or more security level. As shown in step S21 of drawing 12 , a terminal receives this beacon frame. The terminal WL13 which has not joined BSS1, for example, the terminal shown in drawing 1 , can receive a beacon frame.

[0094]

In the receive section 101 of a terminal WL13, the security level of the minimum level of BSS1 written in the beacon frame received as shown in step S22 is taken out, and it is confirmed whether the thing more than the minimum level of BSS1 is in the security level which the terminal WL13 is supporting as shown in step S23. Here, all the security level that the terminal WL13 is supporting may be beforehand registered into the security table of a terminal WL13. When there is nothing more than the minimum level of BSS1 in the security level of a terminal WL13, the connection with a base station AP 1 is stopped, and ends the connection processing.

[0095]

Here, the security level of the minimum level of BSS1 is "enc.1", and since the terminal WL13 is supporting "enc.0" and "enc.1", a terminal WL13 is possible [terminal] for a base station AP 1 and connection. Since there is a thing more than the minimum level of BSS1 in the security level of a terminal WL13, a terminal WL13 chooses the security level this "enc.1", and starts the connection request to a base station AP 1. That is, the security level which progressed to step S2 of drawing 7 , and was chosen is notified, and the same actuation as explanation of the 1st operation gestalt is performed hereafter.

[0096]

However, since it is expectable in this case that the security level more than the

minimum level is surely notified from Terminal WL side, step S3 of drawing 7 may be skipped in a base station AP 1. Moreover, the inside of the security level on which terminal WL13 the very thing has a terminal WL13 in step S2, The security level more than the minimum level of BSS1 notified with the beacon frame is chosen (when there is two or more such security level). all they, some of requests of them, or 1 of them may be chosen, for example, security level may choose the highest thing, the minimum thing, or a desired thing. What is necessary is just to notify to a base station AP 1.

[0097]

Thus, since a terminal WL13 starts connection after choosing beforehand the partner who can connect on the security level which self supports when the base station AP 1 of BSS1 where minimum security level was defined beforehand broadcasts the minimum security level of the BSS concerned, unnecessary traffic is reducible.

[0098]

Moreover, a terminal WL13 can transmit the demand frame (probe request) of probe to a base station AP 1, and a base station AP 1 can also notify security level by the response frame (probe response) of probe to it.

[0099]

(3rd operation gestalt)

Although the operation gestalt of the above 1st explained the case where the authentication and the association which were specified to IEEE802.11 were carried out in this order, carrying out authentication is also assumed after performing an association previously. the case of BSS1 which attached in this case and was shown in drawing 1 with the 3rd operation gestalt -- an example -- ** -- it carries out and explains with reference to the flow chart shown in drawing 13 .

[0100]

Here, the case where the terminal WL13 which has not joined the base station AP 1 of BSS1 at BSS1 requires connection like the 1st operation gestalt is explained, and only a different part from the 1st operation gestalt is explained.

[0101]

That a terminal WL13 should receive the beacon frame transmitted from a base station AP 1 as shown in step S31, and it should connect it to a base station AP 1 after that, as shown in step S32, the demand frame of an association is transmitted to a base station AP 1.

[0102]

As are mentioned above, and shown in the frame of the association of the MAC frame specified to IEEE802.11 at drawing 9 (a), drawing 9 (b), and drawing 9 (c), a free space, i.e., the reserve field, is prepared in "the KYAPA kinky thread tea information (Capabilityinformation)" on the frame body. The transmitting section 107 of a terminal WL13 writes at least one of the security level which is supporting the terminal WL13 in this reserve field of a request in this reserve field, and as shown in step S32, it

transmits to a base station AP 1. For example, in the transmitting section 107 of a terminal WL13, the data in which one "enc.1" in all the security level ("enc.0""enc.1") that self has is shown shall be written in the reserve field, and it shall transmit to a base station AP 1 here.

[0103]

Processing actuation of the base station AP 1 which received this is the same as that of the 1st operation gestalt. That is, the reception-control section 13 of a base station AP 1 compares with the security level of the minimum level of BSS1 which the security level of the terminal WL13 currently written in the received demand frame (Association Request) of an association is registered into drawing, and is registered into the security table 21 of a base station AP 1 in this security level. The security level of this terminal WL13 notified from the terminal WL13 is the security level which is supporting the base station AP 1, and, moreover, it is judged at the time more than the security level of the minimum level in BSS1 that connection of a terminal WL13 is permitted as shown in step S33. Moreover, at the time under of the security level of the minimum level of BSS1, it is judged that connection of a terminal WL13 is refused as shown in step S33. That is, when refusing connection of a terminal WL13, according to a convention of IEEE802.11, as shown in step S34, the code of the purport whose connection is failure is written in the response frame (Status code of Association Response) of an association, and a terminal WL13 is answered. By receiving this frame, a terminal WL13 judges that it was refused by connection from a base station AP 1, and interrupts connection procedure in this phase.

[0104]

On the other hand, when permitting connection of a terminal WL13, for the communication link using "enc.1" which is the security level of the minimum level of BSS1 notified from the terminal WL13, according to a convention of IEEE802.11, the code of the purport whose connection is a success is written in the response frame (Status code of Association Respose) of an association, and as shown in step S36, a terminal WL13 is answered.

[0105]

in response, a terminal WL13 shows to step S37 according to a convention of IEEE802.11 for the authentication processing for sharing a code parameter between a terminal WL13 and a base station AP 1 -- as -- an authentication frame -- transmitting . Processing of the authentication after transmission of an authentication frame is performed according to a convention of IEEE802.11. Since a convention of IEEE802.11 is followed about this processing, that explanation is omitted.

[0106]

In addition, while the effectiveness same [of the 1st operation gestalt] also in this 3rd operation gestalt is expectable, it is not necessary to say that many variations which were explained with the 1st operation gestalt can be applied.

[0107]

(4th operation gestalt)

Next, while a certain terminal moves between the area of two or more base stations, when communicating, the technique of securing each area for every BSS, i.e., security level, is explained taking the case of the wireless LAN system shown in drawing 1 . The technique for securing the minimum security level which was alike to the situation, i.e., BSS to which each base station belongs under the so-called mobile environment, that Terminal WL is moved, respectively, and was defined beforehand is explained in this 4th operation gestalt. As the operation gestalt of the above 1st explained fundamentally, in case the connection request from a terminal is received, the point of performing authentication processing for having security level notified from the terminal concerned, permitting connection of the terminal concerned only when it is more than the minimum security level as which it was beforehand determined to self-BSS, and sharing a code parameter between a base station and a terminal is the same in the base station of each BSS.

[0108]

For example, when the terminal WL13 of drawing 1 has connected with a base station AP 2 and it has moved into the area of a base station AP 1 in the wireless LAN system specified to IEEE802.11, rear sociation (Reassociation) is performed between a terminal WL13 and a base station AP 1. And a data frame is transmitted and received after this rear sociation procedure is completed normally.

[0109]

With this 4th operation gestalt, the security level of a terminal WL13 is notified to a base station AP 1 from a terminal WL13 using a free space in the demand frame (Reassociation Request) of rear sociation.

[0110]

Hereafter, in the wireless LAN system shown in drawing 1 , a terminal WL13 moves to the area of a base station AP 1 from the area of a base station AP 2, and the case where rear sociation is carried out to a base station AP 1 is explained with reference to the flow chart shown in drawing 15 . In addition, in drawing 15 , the same sign is given to the same part as drawing 13 , the explanation is omitted, and a different procedure is explained.

[0111]

As shown in step S31, after receiving the beacon frame transmitted from a base station AP 1, a terminal WL13 transmits the demand frame of rear sociation to a base station AP 1 that it should connect with a base station AP 1, as shown in step S51.

[0112]

As shown in the frame of the rear sociation of the MAC frame specified to IEEE802.11 at drawing 14 (a) - (c), a free space, i.e., the reserve field, is prepared in "Capability information" of the frame body.

[0113]
The transmitting section 107 of a terminal WL13 writes one of the at least requests of the security level which is supporting the terminal WL13 in this reserve field, as shown in step S51, and it transmits to a base station AP 1. For example, in the transmitting section 107 of a terminal WL13, the data in which "enc.1" is shown among all the security level ("enc.0"" enc.1") that self has are written in, and it transmits to a base station AP 1 here.
[0114]
Since processing actuation of the base station AP 1 which received the frame of this rear sociation is the same as explanation of drawing 13 , refer to the explanation about step S33 of drawing 13 for it. However, when refusing connection of a terminal WL13 at step S33, according to a convention of IEEE802.11, the code of the purport whose connection is failure is written in the status code of a rear sociation response frame, and as shown in step S52, a letter is answered by the terminal WL13. Moreover, when permitting connection of a terminal WL13, according to a convention of IEEE802.11, the code of the purport whose connection is a success is written in the status code of a rear sociation response frame, and as shown in step S53, a letter is answered by the terminal WL13.
[0115]
When a base station AP 1 permits connection of a terminal WL13, to share a code parameter is needed between a base station AP 1 and a terminal WL13. Therefore, as shown in step S37 of drawing 15 – step S44, according to a convention of IEEE802.11, the authentication processing for sharing a code parameter between a terminal WL13 and a base station AP 1, i.e., the procedure of authentication, may perform like drawing 13 .
[0116]
Moreover, the address of the base station AP 2 as for which the terminal WL13 is making current connection, i.e., a base station, is described by the demand frame of the rear sociation from a terminal WL13. "The present AP address (Current AP address)" with which this address is shown in drawing 14 (a) – (c) corresponds. Then, as shown in drawing 15 , the procedure of authentication does not perform but a base station AP 1 is connected to a base station AP 2 based on "the present AP address (Current AP address)." And a base station AP 1 requires a transfer of the security information about the terminal WL13 registered into the security table of a base station AP 2, and you may make it register security information into the security table after a transfer of the security information. Thereby, a code parameter is shared between a base station AP 1 and a terminal WL13. Therefore, the data frame enciphered on the same security level can be transmitted [after connection is permitted from the base station AP 1 where a terminal WL13 is shown at step S53 / a terminal WL13] and received between base stations AP 1 like the communication link

between this terminal WL13 and base station AP 2.

[0117]

In addition, in the communication system concerning this 4th operation gestalt, while the same effectiveness is expectable also in the 1st operation gestalt, it is not necessary to say that many variations which were explained with the 1st operation gestalt can be applied.

[0118]

(5th operation gestalt)

as mentioned above, the 1- in the communication system concerning the 4th operation gestalt, it becomes possible to realize a communication link on the security level more than the minimum level as which the terminal WL13 was beforehand determined to BSS1 to which a base station AP 1 belongs between base stations AP 1. However, if the security level of a communication link in the meantime is lower than the minimum level beforehand set to BSS1 when a terminal WL13 communicates with the terminal and other radio stations which have not joined BSS1 other than base station AP1 at the same time a terminal WL13 communicates with a base station AP 1, it cannot be said as a result that the security level of the minimum level of BSS1 was secured. Then, in the communication system concerning this 5th operation gestalt, even if a terminal WL13 carries out a connection request to a base station AP 1 when wireless connection is already made with a certain terminal WL14 as a terminal WL13 shows drawing 16 , according to the procedure explained below, the security of the minimum level beforehand set to BSS1 is securable.

[0119]

When wireless connection of the terminal WL13 is made in other terminals and base stations on the security level with which the minimum security level beforehand set to BSS1 is not filled, it is a base to prevent from connecting a terminal WL13 to the base station or terminal in BSS1. Therefore, in order to connect with the terminal and base station in BSS1, to cut the wireless connection with such low security level beforehand, or to raise the curie tee level of the wireless connection more than the minimum level of BSS1 is needed.

[0120]

the procedure the following and for it -- the 1- explanation is omitted about the common procedure explained with the 4th operation gestalt, and a different procedure is explained.

[0121]

In drawing 16 , the same sign is given to the same part as drawing 1 , and the explanation is omitted. The security level which is supporting the terminal WL14 shown in drawing 16 presupposes that it is "enc.0." In case the demand of the connection of a terminal WL13 with a base station AP 1 is started, wireless connection of the terminal WL13 is already made at a terminal WL14, and

communication link security level in the meantime assumes that it is "enc.0."

[0122]

In such a condition, the case where a terminal WL13 starts a connection request to the base station AP 1 of BSS1 is explained.

[0123]

First, as the 2nd operation gestalt explained, the case where the minimum security level beforehand set to BSS1 with the beacon frame is notified is explained with reference to the flow chart shown in drawing 17 . In this case, a terminal WL13 gets to know that the minimum security level which makes wireless connection is "enc.1" from the received beacon frame to a base station AP 1. Then, a terminal WL13 performs processing actuation shown in drawing 17 , before progressing to step S32 of drawing 13 .

[0124]

In step S61 of drawing 17 , it is checked whether the security level more than minimum level "enc.1" permitted by BSS1 is prepared for the security level of a terminal WL13. When the security level more than "enc.1" is prepared for the terminal WL13, it progresses to step S62. In this step S62, it is confirmed whether be more than minimum level "enc.1" by which the security level of the communication link between the terminal WL14 with which wireless connection of the current terminal WL13 is made, i.e., a terminal, and a terminal WL13 is permitted by BSS1. If it is more than minimum level "enc.1" by which the security level of the communication link between a terminal WL13 and a terminal WL14 is permitted by BSS1, it will progress to step S64 and handshaking between a terminal WL13 and a base station AP 1 will be started. That is, in a terminal WL13, processing after step S32 of drawing 13 is performed. On the other hand, when the security level between a terminal WL13 and a terminal WL14 does not fulfill the minimum level ("enc.1") permitted by BSS1, step S63 HE progress and the wireless connection between a terminal WL13 and a terminal WL14 are cut, and it progresses to step S64.

[0125]

As mentioned above, since the security level of the communication link between a terminal WL13 and a terminal WL14 is "enc.0", it progresses to step S63 from step S62, and the wireless connection between a terminal WL13 and a terminal WL14 is cut. Then, DIO sentimental KESHON (Deauthentication) specified to IEEE802.11 is ended, and a terminal WL13 progresses to step S64.

[0126]

Thus, when a terminal WL13 has the security level lower than the security level broadcast from the base station AP 1 by which a connection request is carried out between the terminals WL14 which are making current connection, the wireless connection between a terminal WL13 and a terminal WL14 is cut beforehand, and a connection request is made a base station AP 1 from a terminal WL13. Therefore,

wireless connection between a terminal WL13 and a base station AP 1 is made certainly, holding the minimum security level of BSS1.

[0127]

In addition, in step S63, once cutting the wireless connection between a terminal WL13 and a terminal WL14, wireless connection of a terminal WL13 and the terminal WL14 may be again made on the security level more than the minimum level of BSS1.

[0128]

Although the explanation mentioned above explained the case where wireless connection of the terminal WL13 was made only with one of the terminals WL14, as well as the above when wireless connection of the terminal WL13 is made in two or more terminal or two or more base stations, each of the security level is checked. If the security level is not more than the minimum level of BSS1, connection between a terminal WL13 and other terminals will once be cut, and a terminal WL13 is set up in security level more than the minimum level of BSS1, and may start connection with a base station AP 1.

[0129]

In addition, although the above-mentioned explanation explained taking the case of the case of a terminal WL14 and the terminal WL13 which is making wireless connection, the procedure of a top Norikazu ream is applicable also to processing actuation of the base station AP 2 of other BSS2 which is different in BSS1. Thus, when both the sides that received the side and connection request which emitted the connection request are not a terminal but base stations, DS communication link from which minimum security level was secured in two or more BSS, respectively is attained. Wireless connection may be made with two or more terminals and a base station in the base station concerned, and when the side which emitted the connection request is a base station, like [in such a case] the above, each of the security level is checked, and as long as it is not a thing more than the minimum level of BSS which it is going to connect from now on, an access point may once cut connection with Terminal WL and other access points. Then, what is necessary is to set up the security level more than the minimum level of BSS which an access point tends to connect after this if needed, and just to make it start connection with the base station of the request concerned after that.

[0130]

Next, as the 1st, 3rd, and 4th operation gestalt explained, the case where the security level of a terminal WL13 is checked is explained with reference to the flow chart shown in drawing 18 in the case of authentication, an association, and rear sociation. In addition, the processing actuation shown in drawing 18 supports step S33 of step S3 of drawing 7 , drawing 13 , and drawing 15 etc.

[0131]

**1 shown below while a terminal WL13 writes the security level of a terminal WL13 in

a free space on the demand frame of authentication, or the demand frame of an association or rear sociation as mentioned above when checking the security level of a terminal WL13 since -- **2 ** -- at least one item is written in the free space or other free space.

[0132]

**1 The terminal with which wireless connection of the current terminal WL13 is made; or existence of a base station.

[0133]

**2 A terminal WL13, the terminal by which current wireless connection is made, or security level between base stations

Here, when wireless connection of the terminal WL13 is made in two or more terminals or base stations, the security level about the all is written in a free space.

[0134]

In a base station AP 1, as shown in step S71, a frame is received, and first, as shown in step S72, the security level of a terminal WL13 is checked. When not filling the minimum security level as which the security level of a terminal WL13 is determined to BSS1, it progresses to step S73 and connection is refused. That is, as the 1st, 3rd, and 4th operation gestalt explained, a connection refusal is notified to a terminal WL13 with the frame of authentication, an association, or rear sociation.

[0135]

On the other hand, when the security level of a terminal WL13 is the security level which a base station AP 1 supports and it is more than the minimum security level moreover set to BSS1 next, it progresses to step S74. Above-mentioned **1 Or **2 When it judges that the terminal or base station which are making current wireless connection do not exist in a terminal WL13 from ******, it progresses to step S75 and wireless connection of a terminal WL13 is permitted. That is, as the 1st, 3rd, and 4th operation gestalt explained, while authorization of wireless connection is notified to a terminal WL13 with the frame of authentication, an association, or rear sociation, it performs similarly with consecutive processing having mentioned above. Step S6 of drawing 7 , step S36 of drawing 13 , and the step S53 grade of drawing 15 are equivalent to this processing. Above-mentioned **1 Or **2 When it judges that the terminal and base station which are making current wireless connection exist in a terminal WL13 from ******, it progresses to step S76.

[0136]

In step S76, to the information received at step S71, **2 When it is alike and shown "the security level between a terminal WL13 and the terminal WL14 which is making current wireless connection" is contained, the security level is checked. When it is more than the minimum security level as which the security level between terminals WL14 is determined to BSS1, it progresses to step S75 and wireless connection of a terminal WL13 is permitted. When the security level between terminals WL14 does not

fulfill the minimum security level set to BSS1, on the other hand, to the information received at step S71 Above-mentioned **2 When it is alike and the shown information is not included (i.e., when the security level between terminals WL14 is unknown), it progresses to step S77 and the connection request from a terminal WL13 is refused. As the 1st, 3rd, and 4th operation gestalt explained, refusal of this connection request is notified to a terminal WL13 with the frame of authentication, an association, or rear sociation.

[0137]

In addition, the purport which refuses a connection request is not notified but you may make it the frame of authentication, an association, or rear sociation notify similarly the demand of a purport with a terminal WL14 which directs cutting of wireless connection at step S77. In this case, it can be judged immediately that a terminal WL13 is connectable with a base station AP 1 if the wireless connection with a terminal WL14 is cut. Therefore, after cutting the wireless connection with a terminal WL14 (for example, after a terminal WL13 ends DIO sentimental KESHON (Deauthentication) specified to IEEE802.11), the connection request of it can be again carried out to a base station AP 1.

[0138]

Moreover, the administrative frame of the MAC frame specified to IEEE802.11 at step S77 after refusing a connection request, Among the frames for control, in the case of a current a non-used frame, for example, an administrative frame You may make it a subtype notify the minimum security level from which a subtype is permitted by BSS1 using frames, such as "0000" - "1001", in the case of frames, such as "0110" - "0111", and the frame for control. If a terminal WL14 can support the minimum security level concerned when there is a notice of the minimum security level permitted by BSS1, a terminal WL13 can perform a connection request to a base station AP 1 again, after reconnecting with the security level.

[0139]

Moreover, the above-mentioned explanation explains taking the case of the case where the terminal WL13 is making wireless connection only with one of the terminals WL14. however, the existence of the terminal which has already connected the terminal WL13 like the above even if it is, when wireless connection is being made with two or more terminals and a base station, or a base station -- each of the security level may be notified preferably. When two or more security level of the radio already connected from the terminal WL13 has been notified, a base station AP 1 should just check the security level about the each in step S76.

[0140]

As mentioned above, when not fulfilling the minimum security level of the side in which it received the connection request when the security level of this wireless connection was unknown even if the side which emitted the connection request was already the

case where wireless connection was being made with other terminals and a base station, the minimum security level of the side which received the connection request can be secured by refusing the connection request concerned. In addition, the above-mentioned explanation is applicable also as processing actuation of the base station AP 2 of other BSS2 which is different in BSS1, although explained taking the case of the case of a terminal WL14 and the terminal WL13 which is making wireless connection. Thus, when both the sides that received the side and connection request which emitted the connection request are not a terminal but base stations, DS communication link from which each minimum security level was secured in two or more BSS is attained. When the side which emitted the connection request is a base station, wireless connection may be made with two or more terminals and a base station in the base station concerned. As for the side which emitted the connection request, it is desirable preferably like [in such a case] the above the existence of the already connected terminal or a base station and to notify each of the security level. What is necessary is just to check the security level about the each in step S76 in the side which received the connection request, when two or more security level of the already connected radio has been notified from the side which emitted the connection request.

[0141]

(6th operation gestalt)

In the wireless system concerning the operation gestalt of the above 1st, although the case where a connection request was carried out to a base station was explained, in the case of the connection request from a terminal to a terminal, the same technique is applicable. Here, as shown in drawing 19 , it explains to the terminal WL12 belonging to BSS1 taking the case of the case where the terminal WL15 which has not joined carries out a connection request to BSS1. The security level which can support a terminal WL15 is "enc.0." Since BSS1 is joined, a terminal WL12 needs to secure the minimum security level beforehand set to BSS1, in case a terminal WL12 communicates. Therefore, the same processing actuation as what was shown in drawing 7 between a terminal and a base station is carried out between a terminal WL12 and a terminal WL15.

[0142]

Drawing 20 shows the procedure between the terminals WL12 and terminals WL15 in the case of carrying out a connection request from a terminal WL15 to a terminal WL12. In addition, in drawing 20 , the same sign is given to the same part as drawing 7 , explanation is omitted, and a point of being below different is explained.

[0143]

In drawing 20 , processing actuation in the base station shown in drawing 7 is equivalent to the processing actuation kicked to a terminal WL12. Therefore, step S1 which a beacon frame transmits is made unnecessary. Other step S2 - step S12 are

the same as that of drawing 7 . In addition, the procedure of an association is made unnecessary.

[0144]

As shown in drawing 20 , the near terminal WL12 which received the connection request also on the occasion of a connection setup between a terminal WL12 and a terminal WL15 is checking the security level of the terminal WL15 of the side which emitted the connection request. Here, the security level of the terminal of the side which emitted the connection request is the security level which the near equipment which received the connection request supports, and if it is more than the minimum security level of BSS1 to which the near terminal which received the connection request moreover belongs, connection of a terminal WL15 will be permitted. If it is below the minimum security level of BSS1 to which the near terminal which is not the security level which the near equipment with which the security level of the terminal of the side which emitted the connection request received the connection request supports, or received the connection request belongs, connection of a terminal WL15 will be refused. If connection is authorization, manual processing actuation for sharing the code parameter corresponding to the security level concerned will be performed.

[0145]

In addition, when a terminal WL12 receives a connection request from a terminal WL13, a terminal WL12 performs processing actuation as shown in drawing 20 irrespective of whether the terminal WL12 is making wireless connection with the base station AP 1.

[0146]

In drawing 19 , the mode in which a terminal WL15 transmits a direct data frame to a terminal WL12 may be applied. This mode is called ad hoc (ad hoc) mode. This ad hoc mode can be performed without passing through authentication. Ad hoc mode is explained about processing actuation with a terminal WL12 with reference to the flow chart shown in drawing 21 .

[0147]

A terminal WL12 receives the data frame addressed to the direct terminal WL12, without minding a base station from a terminal WL15, as shown in step S81. According to the convention of IEEE802.11, such a data frame can be easily judged from both "To DS" and "From DS" under frame control of the MAC frame shown in drawing 4 being "0."

[0148]

In the receive section 101 of a terminal WL12, when this data frame is received, it is confirmed whether as shown in step S82, the security information corresponding to the address of that transmitting origin is registered into the security table 110 of a terminal WL12.

[0149]

It means what is defined beforehand that it is the security level more than the

minimum level as which the terminal WL15 was beforehand determined to BSS1 registered into the terminal WL12 and the security table concerned that the security information of a terminal WL15 is registered into the security table, and it had communicated in the past, or communicates on such security level. Therefore, it progresses to step S83, and a terminal WL12 transmits the ACK frame to the data frame which the convention received to EEE802.11 to a terminal WL15, and starts transmission and reception of the data between terminals WL15.

[0150]

On the other hand, in step S82, since the security level of a terminal WL15 is unknown as [this] when the security information of a terminal WL15 is not registered into a security table, between terminals WL15, the communication link of a terminal WL12 is impossible. Therefore, it progresses to step S84 and the above-mentioned ACK frame notifies the purport which requires authentication of the terminal WL15 concerned, without transmitting. You may make it a subtype notify [a subtype] this notice the case of a current a non-used frame, for example, an administrative frame, using frames, such as "0000" - "1001", among the administrative frame of the MAC frame specified to IEEE802.11, and the frame for control in the case of frames, such as "0110" - "0111", and the frame for control.

[0151]

The terminal WL15 which received this notice should just start the processing actuation after step S2 shown in drawing 20 . In step 84 mentioned above, a terminal WL12 transmits the ACK frame and the step which a terminal WL15 starts processing of step S2, and shows after that to drawing 20 may be performed.

[0152]

By the communication procedure concerning the operation gestalt of the above 5th, as shown in drawing 16 , when the terminal WL13 had already made wireless connection with a certain terminal WL14 and a connection request was carried out to a base station AP 1, the technique for securing the security of the minimum level beforehand set to BSS1 of a base station AP 1 was explained. As shown in drawing 22 , when the terminal WL15 has already made wireless connection with a certain terminal WL16 corresponding to this next, the case where this terminal WL15 carries out a connection request to a terminal WL12 is explained.

[0153]

Here, the security level which can support a terminal WL16 is "enc.0." Since BSS1 is joined, a terminal WL12 needs to secure the minimum security level beforehand set to BSS1, in case a terminal WL12 starts a communication link. For that purpose, what is necessary is just made to carry out the same processing actuation as what was shown in drawing 18 at a terminal WL12.

[0154]

Drawing 23 shows the procedure between the terminals WL12 and terminals WL15 in

the case of carrying out a connection request from a terminal WL15 to a terminal WL12. In addition, in drawing 23 , the same sign is given to the same part as drawing 18 , the explanation is omitted, and a different part is explained. That is, in drawing 23 , the processing actuation in the base station and terminal WL13 of drawing 18 is equivalent to the processing actuation in a terminal WL12 and a terminal WL15, respectively, and the same, same processing as the procedure substantially shown in drawing 18 is carried out. Therefore, if the base station and terminal WL13 under above-mentioned explanation in drawing 18 transpose to a terminal WL12 and a terminal WL15 about the explanation which refers to drawing 23 , respectively, it is not necessary to explain especially and you can understand.

[0155]

Moreover, in drawing 22 , also when it is going to transmit a direct data frame to a terminal WL12, without a terminal WL15 passing through authentication, a terminal WL12 may be made to carry out processing actuation as shown in drawing 23 , after carrying out processing actuation of the flow chart of drawing 21 . It is desirable to carry out processing actuation which the terminal WL12 was step S81 of drawing 21 preferably, and progressed to step S84 immediately, notified the purport which requires authentication of the terminal WL15 concerned, and was surely shown in drawing 23 when the data frame addressed to the direct terminal WL12, without minding a base station was received from a terminal WL15, when securing security. The terminal WL15 since the security information of a terminal WL15 is registered into the security table of a terminal WL12 is because it does not necessarily communicate above the minimum security level of BSS1 to which a terminal WL12 belongs to the wireless connection with terminals other than terminal WL12.

[0156]

in addition, the existence of the terminal which has already connected the terminal WL15 as well as the above when wireless connection is being made with two or more terminals or a base station, although the above-mentioned explanation explained the case where the terminal WL15 was making wireless connection only with one of the terminals WL16 to the example, or a base station -- each of the security level is notified preferably. When two or more security level of the radio already connected from the terminal WL15 has been notified, a terminal WL12 should just check the security level about the each in step S76.

[0157]

As explained above, when the security level which one of them should protect at worst is a terminal in BSS defined beforehand also in the communication link between two or more terminals according to the operation gestalt of the above 6th, the security level concerned can be secured.

[0158]

(7th operation gestalt)

above-mentioned the 1- the 6th operation gestalt explained the case where the security level of BSS was secured. In IBSS, the same technique can be applied, also when securing security level.

[0159]

This 7th operation gestalt explains taking the case of IBSS1 of a configuration as shown in drawing 24 .

[0160]

In drawing 24 , IBSS1 consists of plurality WL31-WL33, for example, three terminals. A terminal WL31 supports security level "enc.0" and "enc.1", a terminal WL32 shall support security level "enc.0", "enc.1", and "enc.2", and a terminal WL33 shall support security level "enc.0" and "enc.1."

[0161]

IBSS can transmit [according to the convention of IEEE802.11] and receive a direct data frame, without passing through the authentication process of authentication between the terminals of the plurality in IBSS without minding a base station. Each terminal in IBSS1 has a security table, the security information of each terminal which constitutes IBSS1 on this security table is registered, and if it is made to communicate above the minimum security level beforehand defined within IBSS1, between the terminals in IBSS1, that minimum security level is securable.

[0162]

Then, the processing actuation when having not joined one [WL31] of two or more terminals which constitute IBSS1, for example, a terminal, at IBSS1, namely, receiving a connection request from the terminal WL34 which is not registered into a security table is explained.

[0163]

This processing actuation as well as the 6th operation gestalt transmits the notice of the purport which requires authentication to a terminal WL34 the transmitting origin of the data frame concerned, when a terminal WL31 carries out processing actuation as showed preferably drawing 21 and the security information of the transmitting origin of the received data frame is not registered into an own security table. Then, transmission of the frame of authentication carries out processing actuation as shown in drawing 23 preferably from a terminal WL34. However, the terminal WL15 shown in drawing 23 should just be transposed to a terminal WL34. While a terminal WL34 writes the security level of a terminal WL34 in the frame of authentication, namely, above-mentioned **1 since -- **2 ** -- at least one is written in and it transmits to a terminal WL31. A terminal WL31 receives the frame of such authentication from a terminal WL34, and the same processing actuation as the terminal WL12 shown in drawing 23 should just be carried out.

[0164]

Thus, also in IBSS, the minimum security level beforehand set to the IBSS is

securable.

[0165]

Moreover, also in the communication link between two or more terminals, when the security level which one of them should protect at worst is a terminal in IBSS defined beforehand, the security level concerned can be secured.

[0166]

the above the 1- as the 7th operation gestalt explained, the radio communication equipment which constitutes wireless LAN, such as a base station and a terminal, respectively By having at least one security level (preferably plurality), and having the description shown in following - (x1) (x8) For example, the radio which secured the minimum security level by the encryption beforehand defined for every basic group of wireless LAN, such as BSS and IBSS, i.e., a communication link group, is realizable. Moreover, in the communication link between two or more radio communication equipments, when it is a radio communication equipment in the security level which at least one of two or more of the radio communication equipments concerned should protect at worst and the communication link group by whom the security level of the minimum level is beforehand defined if it puts in another way, for example, BSS, and IBSS, the security level more than the above-mentioned minimum level can surely be secured. In addition, it is the function which should have a base station and a terminal in common preferably about the description which is not clearly written to be the case where it is especially a base station in the following (x1) - (x8).

[0167]

(x1) In case a connection request is carried out from self-equipment to the 1st radio communication equipment which is other radio communication equipments, notify the 1st security level which is the security level used by the communication link between this 1st radio communication equipment among the security level which self-equipment has at least one to said 1st radio communication equipment.

[0168]

(x2) In case a connection request is carried out to said 1st radio communication equipment, when self-equipment has already connected with the 2nd radio communication equipment which is other radio communication equipments other than said 1st radio communication equipment, notify the 2nd security level which is the security level used by the communication link between this 2nd radio communication equipment.

[0169]

(x3) When said 1st radio communication equipment is a base station and the security level of the minimum level connectable with this 1st radio communication equipment is broadcast, choose the security level more than this minimum level among the security level which self-equipment has, and in case the connection request of it is carried out to said 1st radio communication equipment, notify.

[0170]

(x4) When said 1st radio communication equipment is a base station and two or more security level connectable with this 1st radio communication equipment is broadcast, choose a match as either of two or more security level this broadcast among the security level which self-equipment has, and in case the connection request of the selected security level is carried out to said 1st radio communication equipment, notify.

[0171]

(x5) When self-equipment receives a connection request from the 4th radio communication equipment which is other radio communication equipments, The 3rd security level which is the security level used at least by the communication link between this 4th radio communication equipment and self-equipment which were notified from this 4th radio communication equipment is in the security level which self-equipment has. A -- and when it is more than the minimum level beforehand set to the communication link group (namely, BSS and IBSS) to whom self-equipment belongs connection of this 4th radio communication equipment -- granting a permission -- (b) -- at least when said 3rd security level does not fulfill this minimum level, 3rd means to refuse connection with this 4th radio communication equipment is provided.

[0172]

(x5') While the security level of the A above 3rd is more than the minimum level beforehand set to the communication link group to whom self-equipment belongs, said 3rd means When said 4th radio communication equipment has already connected with the 5th radio communication equipment which is other radio communication equipments other than said 4th radio communication equipment When the 4th security level which is the security level used by the communication link between the 5th radio communication equipment concerned is said more than minimum level When permitting connection with this 4th radio communication equipment and not filling the security level of the (b) above 3rd more than said minimum level, Or when said 4th radio communication equipment has already connected with said 5th radio communication equipment, and said 4th security level is unknown, connection with said 4th radio communication equipment is refused [when said 4th security level does not fulfill said minimum level, or].

[0173]

(x7) When self-equipment is a base station, provide 4th means to broadcast the security level of the minimum level beforehand set to the communication link group to whom self-equipment belongs, or two or more security level more than this minimum level.

[0174]

(x8) If there is a thing more than the minimum level beforehand set to the

communication link group to whom self-equipment belongs to two or more of the security level when two or more security level has been notified from said 4th radio communication equipment, choose one of them and provide 5th means to notify it to said 4th radio communication equipment.

[0175]

The technique of this invention indicated in the gestalt of implementation of this invention can also be stored and distributed to record media, such as magnetic disks (a floppy disk, hard disk, etc.), optical disks (CD-ROM, DVD, etc.), and semiconductor memory, as a program which a computer can be made to execute.

[0176]

[Effect of the Invention]

As explained above, according to this invention, radio which secured minimum security level by the encryption beforehand set into each group to every [of wireless LAN] basic group (communication link group), such as BSS and IBSS, can be performed. Moreover, when the security level (security level of the minimum level) which at least one of two or more radio communication equipments concerned should protect at worst is a wireless radio communication equipment in the communication link group (for example, BSS and IBSS) set beforehand in the communication link between two or more radio communication equipments, the security level more than the above-mentioned minimum level is surely **.

****** -- things are made.

[Brief Description of the Drawings]

[Drawing 1] It is the mimetic diagram showing roughly the communication system concerning the operation gestalt of this invention.

[Drawing 2] It is the block diagram showing an example of the circuitry of the base station shown in drawing 1 .

[Drawing 3] It is the block diagram showing an example of the circuitry of the wireless terminal shown in drawing 1 .

[Drawing 4] It is the mimetic diagram showing the structure of the MAC frame specified to IEEE802.11 transmitted between the base stations and terminals in the communication system shown in drawing 1 .

[Drawing 5] It is the table showing one example of the security table with which the base station or terminal in the communication system shown in drawing 1 is equipped.

[Drawing 6] The base station or terminal in the communication system shown in drawing 1 is the table showing other examples of a security table.

[Drawing 7] It is a flow chart for explaining an example of processing actuation of the base station in the communication system shown in drawing 1 , and a terminal.

[Drawing 8] The mimetic diagram having shown the frame structure of the authentication specified to IEEE802.11 transmitted between the base stations and terminals in the communication system which shows (a) to drawing 1 , and (b) are the tables showing the contents described by the item of the frame shown in (a).

[Drawing 9] (a) - (c) is the mimetic diagram having shown the structure of the association request frame specified to IEEE802.11 transmitted between the base stations and terminals in the communication system shown in drawing 1 , and an association response frame.

[Drawing 10] It is the table showing the example of the updated security table with which the base station or terminal in the communication system shown in drawing 1 is equipped.

[Drawing 11] It is the mimetic diagram showing the structure of the beacon frame specified to IEEE802.11 turned to a terminal from the base station in the communication system shown in drawing 1 .

[Drawing 12] It is the flow chart which shows the processing procedure which the security level of the minimum level beforehand set to BSS to which a base station belongs to a terminal from the base station in the communication system shown in drawing 1 is notified, and carries out a connection request to a base station.

[Drawing 13] It is the flow chart which shows the processing procedure by which security level is notified using the association response frame transmitted between the base stations and terminals in the communication system shown in drawing 1 , and this security level is checked.

[Drawing 14] (a) - (c) is the mimetic diagram having shown the structure of the rear sociation request frame specified to IEEE802.11 transmitted between the base stations and terminals in the communication system shown in drawing 1 , and a rear sociation response frame.

[Drawing 15] It is the flow chart which shows the processing procedure by which security level is notified using the rear sociation response frame transmitted between the base stations and terminals in the communication system shown in drawing 1 , and this security level is checked.

[Drawing 16] It is the block diagram showing roughly the communication system concerning other operation gestalten of this invention.

[Drawing 17] In the communication system shown in drawing 16, it is a flow chart for explaining an example of the processing procedure of the side which emitted the connection request at the time of the radio communication equipment connected to other radio communication equipments carrying out a connection request to the radio communication equipment of further others.

[Drawing 18] In the communication system shown in drawing 16, it is a flow chart for explaining an example of the processing procedure of the side which emitted the connection request at the time of the radio communication equipment connected to

other radio communication equipments carrying out a connection request to the radio communication equipment of further others.

[Drawing 19] It is the block diagram showing roughly the communication system concerning the operation gestalt of further others of this invention.

[Drawing 20] It is a flow chart for explaining the procedure for making wireless connection between the terminals in the communication system shown in drawing 19.

[Drawing 21] It is a flow chart for explaining an example of processing actuation with the terminal at the time of making wireless connection between the terminals in the communication system shown in drawing 19.

[Drawing 22] It is the block diagram showing roughly the communication system concerning the operation gestalt of further others of this invention.

[Drawing 23] It is a flow chart for explaining other examples of processing actuation with the terminal for making wireless connection between the terminals in the communication system shown in drawing 22.

[Drawing 24] It is the block diagram showing roughly the communication system concerning the operation gestalt of further others of this invention.

[Description of Notations]

AP1, AP2 -- Base station (base transceiver station equipment)

WL11-WL16, WL31-WL34 -- Terminal (wireless terminal unit)

11 -- Receiver

12 -- Transmitter

13 -- Reception-control section

14 -- Transmission-control section

20,100 -- Antenna

21,110 -- Security table

101 -- Receive section

107 -- Transmitting section

108 -- Information processing section

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-32664
(P2004-32664A)
(43)公開日　平成16年1月29日(2004.1.29)

(51)Int.Cl.[7]	F I		テーマコード（参考）
H04L 12/28	H04L 12/28	300Z	5K033
H04Q 7/38	H04B 7/26	109R	5K067

審査請求 未請求　請求項の数 25　OL　（全 39 頁）

(21)出願番号　特願2002-378650(P2002-378650)
(22)出願日　平成14年12月26日(2002.12.26)
(31)優先権主張番号　特願2001-395475(P2001-395475)
(32)優先日　平成13年12月26日(2001.12.26)
(33)優先権主張国　日本国(JP)

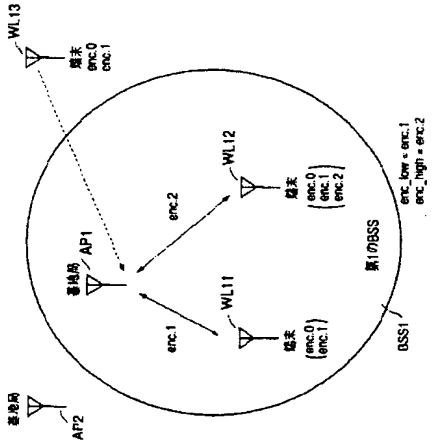
（特許庁注：以下のものは登録商標）
フロッピー

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100058479
弁理士　鈴江　武彦
(74)代理人　100084618
弁理士　村松　貞男
(74)代理人　100068814
弁理士　坪井　淳
(74)代理人　100092196
弁理士　橋本　良郎
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠

最終頁に続く

(54)【発明の名称】無線通信システム及び無線通信装置並びに無線通信方法

(57)【要約】
【課題】通信グループで予め定められた暗号化による最低限のセキュリティレベルを確保して無線通信が可能な無線通信装置を提供するにある。
【解決手段】通信システムにおいて、通信グループに属する第１の無線通信装置は、この通信グループ外の第２の無線通信装置から通知セキュリティレベルを含む接続要求フレームを受信する。第１の無線通信装置は、非暗号化を含む暗号化方法及びその強さに依存して定まるセキュリティレベルから選定された前記無線通信グループに特有の基準セキュリティレベルをその内に格納している。第１の無線通信装置において、通知セキュリティレベルが基準セキュリティレベルと比較されて第２の無線通信装置との接続を拒否する接続拒否或いは第２の無線通信装置との接続を許可する接続許可が記述された応答フレームが発生され、第２の無線通信装置に送信される。



1

【特許請求の範囲】
【請求項１】
通知セキュリティレベルが記述された第１のフィールドを有する第１の送信フレームを通信グループ外の無線通信装置から受信する受信部と、
非暗号化を含む暗号化方法及び暗号化の強さに依存するセキュリティレベルから選定され、前記無線通信グループに割り当てられた基準セキュリティレベルを記憶するメモリ部と、
前記通知セキュリティレベルを前記基準セキュリティレベルと比較して前記無線通信グループ外の無線通信装置との接続拒否或いは接続許可を決定し、決定された接続拒否或いは接続許可が記載される第２のフィールドを有する第２の送信フレームを発生するフレーム発生部と、及び
この第２の送信フレームを前記無線通信グループ外の無線通信装置に向けて送信する送信部と、
を具備することを特徴とする前記無線通信グループに属する無線通信装置。
【請求項２】
前記基準セキュリティレベルは、第１、第２及び第３のセキュリティレベルから選定され、前記第１のセキュリティレベルが非暗号化に相当し、前記第２のセキュリティレベルが第１の暗号化における第１の暗号化の強さに相当し、前記第３のセキュリティレベルが前記第１の暗号化における第２の暗号化の強さに相当することを特徴とする請求項１の無線通信装置。
【請求項３】
前記フレーム発生部は、前記通知セキュリティレベルが前記基準セキュリティレベルよりも低ければ接続拒否を決定し、前記通知セキュリティレベルが前記基準セキュリティレベルよりも低くなければ接続許可を決定することを特徴とする請求項１の無線通信装置。
【請求項４】
前記接続許可の場合には、前記メモリ部が前記無線通信グループ外の無線通信装置のアドレス及び前記通知セキュリティレベルを保持することを特徴とする請求項１の無線通信装置。
【請求項５】
前記第２の通信フレームは、前記無線通信グループを特定するアドレスが記述された第３のフィールドを含むことを特徴とする請求項１の無線通信装置。
【請求項６】
無線通信グループに属する第１の無線通信装置及びこの無線通信グループ外の第２の無線通信装置から構成される無線通信システムにおいて、前記第１の無線通信装置は、
通知セキュリティレベルが記述された第１のフィールドを有する第１の送信フレームを前記第２の無線通信装置から受信する受信部と、

2

非暗号化を含む暗号化方法及び暗号化の強さに依存するセキュリティレベルから選定され、前記無線通信グループに割り当てられた基準セキュリティレベルを記憶する第１のメモリ部と、
前記通知セキュリティレベルを前記基準セキュリティレベルと比較して前記第２の無線通信装置との接続拒否或いは接続許可を決定し、決定された接続拒否或いは接続許可が記載される第２のフィールドを有する第２の送信フレームを発生する第１のフレーム発生部と、及び
この第２の送信フレームを前記第２の無線通信装置に向けて送信する送信部と、
を具備することを特徴とする無線通信システム。
【請求項７】
前記基準セキュリティレベルは、第１、第２及び第３のセキュリティレベルから選定され、前記第１のセキュリティレベルが非暗号化に相当し、前記第２のセキュリティレベルが第１の暗号化における第１の暗号化の強さに相当し、前記第３のセキュリティレベルが前記第１の暗号化における第２の暗号化の強さに相当することを特徴とする請求項６の無線通信システム。
【請求項８】
前記第１のフレーム発生部は、前記通知セキュリティレベルが前記基準セキュリティレベルよりも低ければ接続拒否を決定し、前記通知セキュリティレベルが前記基準セキュリティレベルよりも低くなければ接続許可を決定することを特徴とする請求項６の無線通信システム。
【請求項９】
前記接続許可の場合には、前記第１のメモリ部が前記第２の無線通信装置のアドレス及び前記通知セキュリティレベルを保持することを特徴とする請求項６の無線通信システム。
【請求項１０】
前記第２の通信フレームは、前記無線通信グループを特定するアドレスが記述された第３のフィールドを含むことを特徴とする請求項６の無線通信システム。
【請求項１１】
前記第２の無線通信装置は、前記基準セキュリティレベル及び前記第１の無線通信グループのアドレスを保持する第２のメモリ部を具備することを特徴とする請求項６の無線通信システム。
【請求項１２】
接続拒否が記述される第２のフィールドを有する第２の送信フレームを前記第２の無線通信装置が受信した場合には、前記第２の無線通信装置は、第２の通知セキュリティレベルが記述された第４のフィールドを有する第３の送信フレームを前記第１の無線通信装置に送信することを特徴とする請求項６の無線通信システム。
【請求項１３】
前記第１のメモリは、前記第１の無線通信装置でサポートされるセキュリティレベル及び暗号化レベルに関連す

る暗号化パラメータを保持し、前記基準セキュリティレベルがこのサポートされているセキュリティレベルから選定されることを特徴とする請求項６の無線通信システム。

【請求項１４】

接続許可が記述される第２のフィールドを有する第２の送信フレームを前記第２の無線通信装置が受信した場合には、前記第２の無線通信装置は、暗号化データが格納されている第５のフィールドを有する第４の送信フレームを前記第１の無線通信装置に送信し、前記第１の無線通信装置が前記暗号化パラメータを用いて暗号化データを複合化することを特徴とする請求項１３の無線通信システム。

【請求項１５】

前記第１の送信フレームは、前記第１の無線通信装置でサポートされている複数の通知セキュリティレベルが記載された第１のフィールドを有し、前記フレーム発生部が前記通知セキュリティレベルの夫々を前記基準セキュリティレベルと比較し、前記通知セキュリティレベルの全てが前記基準セキュリティレベルよりも低ければ接続拒否を決定し、前記通知セキュリティレベルの１つが前記基準セキュリティレベルよりも低くなければ接続許可を決定することを特徴とする請求項１３の無線通信システム。

【請求項１６】

前記通知セキュリティレベルは、前記第２の無線通信装置がサポートする通知セキュリティレベル中の最大のレベルに相当することを特徴とする請求項６の無線通信システム。

【請求項１７】

前記無線通信グループ外の第３の無線通信装置であって前記通知セキュリティレベルで前記第２の無線通信装置と通信している第３の無線通信装置を更に具備することを特徴とする請求項６の無線通信システム。

【請求項１８】

前記無線通信グループに属する第３の無線通信装置であって前記基準セキュリティレベルより低くないセキュリティレベルで前記第２の無線通信装置と通信している第３の無線通信装置を更に具備することを特徴とする請求項６の無線通信システム。

【請求項１９】

前記第１及び第３の無線通信装置の１つは、アクセスポイントに相当することを特徴とする請求項６の無線通信システム。

【請求項２０】

前記第１及び第３の無線通信装置の１つは、無線端末に相当することを特徴とする請求項６の無線通信システム。

【請求項２１】

前記第２及び第３の無線通信装置の１つは、無線端末に

相当することを特徴とする請求項６の無線通信システム。

【請求項２２】

前記無線通信グループ外の第３の無線通信装置であって前記通知セキュリティレベルで前記第２の無線通信装置と通信している第３の無線通信装置と、

前記無線通信グループに属する第４の無線通信装置であって前記基準セキュリティレベルより低くないセキュリティレベルで前記第２の無線通信装置と通信している第４の無線通信装置を更に具備することを特徴とする請求項６の無線通信システム。

【請求項２３】

前記第１の無線通信装置がビーコンフレームを第２の無線通信装置に通知して前記第１の送信フレームの送信を要求し、前記ビーコンフレームは、前記第１の無線通信装置でサポートし、前記基準セキュリティレベルより低くないセキュリティーフレームが記載されたフィールドを有することを特徴とする請求項６の無線通信システム。

【請求項２４】

前記第２の無線通信装置は、前記通知セキュリティレベルを含む第２のセキュリティレベルを記憶する第２のメモリ部と、

前記第２のセキュリティレベルを前記基準セキュリティレベルと比較して前記通知セキュリティレベルとして１つのセキュリティレベルを決定して前記第１の送信フレームを発生する第２のフレーム発生部と、及び

及び

この第１の送信フレームを第１の無線通信装置に向けて送信する送信部と、

を更に具備することを特徴とする請求項６の無線通信システム。

【請求項２５】

通知セキュリティレベルが記述された第１のフィールドを有する第１の送信フレームを通信グループ外から受信し、

非暗号化を含む暗号化方法及び暗号化の強さに依存するセキュリティレベルから選定され、前記無線通信グループに割り当てられた基準セキュリティレベルを記憶し、

前記通知セキュリティレベルを前記基準セキュリティレベルと比較して前記無線通信グループ外の無線通信装置との接続拒否或いは接続許可を決定し、決定された接続拒否或いは接続許可が記載される第２のフィールドを有する第２の送信フレームを発生し、及び

この第２の送信フレームを前記無線通信グループ外の無線通信装置に向けて送信することを特徴とする無線通信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

5

この発明は、無線通信システム及び無線通信装置並びに無線通信方法に係り、特に、複数の無線端末装置及びアクセスポイントから構成される無線通信システムに関する。

【０００２】

【従来の技術】

無線ＬＡＮとして、ＩＥＥＥ８０２．１１（ＩＥＥＥ８０２．１１システムは、ＩＥＥＥ８０２．１１ａシステム及びＩＥＥＥ８０２．１１ｂシステム等を含むものとする。）に基づく無線ＬＡＮシステムが非特許文献１で知られている。この無線ＬＡＮシステムでは、暗号化方式として有線と同様にプライバシーを確保することができるＷＥＰ（Ｗｉｒｅｄ　Ｅｑｕｉｖａｌｅｎｔ　Ｐｒｉｖａｃｙ）という方式が適用されている。従って、ＩＥＥＥ８０２．１１に基づく無線ＬＡＮのセキュリティレベルには、ＷＥＰが適用されるＷＥＰモード及びＷＥＰが適用されない非ＷＥＰモードがある。

【０００３】

実際のＩＥＥＥ８０２．１１に従った無線ＬＡＮの製品においては、ＷＥＰという暗号化方式が適用されるＷＥＰモード及び適応されない非ＷＥＰモードの何れかでの通信が可能であり、また、ＷＥＰが適用されるＷＥＰモードにおいては、暗号化のレベルが異なる６４ビット及び１２８ビットの暗号化モードがあり、いずれかが無線ＬＡＮにおける各通信或いは各接続リンクに適用されて通信が実現される。ここで、暗号化のレベルが高ければ高いほど、セキュリティレベルが高く、より強く暗号化されていることを意味している。

【０００４】

ＩＥＥＥ８０２．１１に従った無線ＬＡＮの一形態として、１台のアクセスポイント（以下、基地局とも称する。）及びこのアクセスポイントに接続される複数の無線クライアント（以下、端末とも称する。）から構成されるＢＳＳ（Ｂａｓｉｃ　Ｓｅｒｖｉｃｅ　Ｓｅｔ）という構成単位があり、複数のＢＳＳが用意されてネットワークが構築されるシステムがある。

【０００５】

このＢＳＳ間を接続する構造的な要素は、ＤＳ（Ｄｉｓｔｒｉｂｕｔｉｏｎ　Ｓｙｓｔｅｍ）と称せられている。基地局、即ち、アクセスポイントは、このＤＳに接続する機能を有し、情報は、アクセスポイントを介してＢＳＳとＤＳとの間を伝達される。従って、端末は、アクセスポイントを介して他のＢＳＳに属する端末とも通信することができる。

【０００６】

端末は、ＢＳＳに属し、基地局を介して他のＢＳＳに属する端末と通信するためには、基地局との間でオーセンティケーション（ａｕｔｈｅｎｔｉｃａｔｉｏｎ）及びアソシエーション（ａｓｓｏｃｉａｔｉｏｎ）手続きが実施される。また、端末が他のアクセスポイントに無線

6

接続し直すときにはリアソシエーション（ｒｅａｓｓｏｃｉａｔｉｏｎ）手続きが実行される。

【０００７】

ＩＥＥＥ８０２．１１に定まる無線ＬＡＮでは、交換するフレームの種類として、アクセス制御の為の制御用フレーム（ｃｏｎｔｒｏｌ　ｆｒａｍｅ）と、ビーコンをはじめとする管理用フレーム（ｍａｎａｇｅｍｅｎｔ　ｆｒａｍｅ）と、データ通信用のデータフレーム（ｄａｔａ　ｆｒａｍｅ）とがある。ここで、オーセンティケーション、アソシエーション及びリアソシエーションの処理には、管理用フレームが使用される。

【０００８】

端末がアクセスポイントとの間でデータフレームを送受する場合には、必ずその前にオーセンティケーション及びアソシエーション処理が実行される。

【０００９】

ＩＥＥＥ８０２．１１に定まる無線ＬＡＮでは、端末が暗号化方式であるＷＥＰを使用するか否かを基地局に問い合わせる。即ち、オーセンティケーション要求（ａｕｔｈｅｎｔｉｃａｔｉｏｎ　ｒｅｑｕｅｓｔ）において、端末が基地局にＷＥＰを使用することを要求し、この要求を受けた基地局は、ＷＥＰを使用できる場合には、基地局と端末との間でオーセンティケーションフレームを送受している。このようなオーセンティケーションフレームの送受に基づいてＷＥＰを使用できるようになる。

【００１０】

ＩＥＥＥ８０２．１１に定まる無線ＬＡＮの他の形態として、既存のインフラとは独立に存在するＢＳＳがあり、これをＩＢＳＳ（Ｉｎｄｅｐｅｎｄｅｎｔ　Ｂａｓｉｃ　Ｓｅｒｖｉｃｅ　Ｓｅｔ）と称している。ＩＢＳＳでは、アクセスポイントは、用意されず、ＩＢＳＳは、端末が直接互いに通信し合う通信形態に相当している。また、ＩＢＳＳでは、アソシエーション処理は、実行されず、同様に、リアソシエーション処理も実行されない。このＩＢＳＳでは、端末間でオーセンティケーション処理を経ていなくてもデータフレームを送受することができる。

【００１１】

【非特許文献１】ＩＳＯ／ＩＥＣ　８８０２－１１：１９９９（Ｅ）　ＡＮＳＩ／ＩＥＥＥ　Ｓｔｄ　８０２．１１、１９９９　ｅｄｉｔｉｏｎ

【００１２】

【発明が解決しようとする課題】

このように、従来の無線ＬＡＮでは、セキュリティ対策の１つとして通信データが暗号化されている。通信に際して暗号化機能（ＷＥＰ機能）を用いるか否かは、接続要求を発した側、例えば、端末から接続要求を受けた側、例えば、アクセスポイントに要求される。この要求を受けた基地局側では、当該要求に合ったＷＥＰ機能の

使用が可能であれば、当該要求を受け入れ、当該端末との間でのデータ通信を暗号化している。また、何れのセキュリティレベルで通信を実施するかも接続要求を発した側で主導的に定められる。

【００１３】

今後、無線ＬＡＮには、ＷＥＰ以外にも、ＷＥＰよりセキュリティレベルの高い暗号化方式など、暗号化のレベルが異なる複数種類の暗号化方式が無線ＬＡＮに採用されると推測される。従って、暗号化方式の種類、暗号化レベルなどに応じてきめ細かなセキュリティレベルの設定が可能となることが要求される。

【００１４】

しかし、従来の無線ＬＡＮでは、ＢＳＳ毎に、セキュリティ確保のために最低の暗号化レベルが予め定め、それ以上のレベルを有する暗号化での通信しか許容しないシステムを作るということができないばかりか、通信の際に、暗号化方式の種類、暗号化強度などに応じたきめ細やかなセキュリティレベルが設定できない問題点がある。

【００１５】

さらに、ＩＢＳＳではデータフレームを送信する際にオーセンティケーションをする必要がないため、暗号化されないデータフレームを送信してシステム内のセキュリティを確保することができない問題点がある。

【００１６】

また、ＢＳＳ毎に、そのＢＳＳに予め定められたセキュリティレベルを確保することができないと同様に複数のＢＳＳ間で通信するＤＳ通信においても、各ＢＳＳに定められたセキュリティレベルを確保することはできない問題点がある。

【００１７】

この発明は上述した事情に鑑みなされたものであって、その目的は、通信グループで予め定められた暗号化による最低限のセキュリティレベルを確保して無線通信ができる無線通信システム及び無線通信装置並びに無線通信方法を提供するにある。

【００１８】

【課題を解決するための手段】

この発明によれば、

通知セキュリティレベルが記述された第１のフィールドを有する第１の送信フレームを通信グループ外の無線通信装置から受信する受信部と、

非暗号化を含む暗号化方法及び暗号化の強さに依存するセキュリティレベルから選定され、前記無線通信グループに割り当てられた基準セキュリティレベルを記憶するメモリ部と、

前記通知セキュリティレベルを前記基準セキュリティレベルと比較して前記無線通信グループ外の無線通信装置との接続拒否或いは接続許可を決定し、決定された接続拒否或いは接続許可が記載される第２のフィールドを有

する第２の送信フレームを発生するフレーム発生部と、及び

この第２の送信フレームを前記無線通信グループ外の無線通信装置に向けて送信する送信部と、

を具備することを特徴とする前記無線通信グループに属する無線通信装置が提供される。

【００１９】

また、この発明によれば、

無線通信グループに属する第１の無線通信装置及びこの無線通信グループ外の第２の無線通信装置から構成される無線通信システムにおいて、前記第１の無線通信装置は、

通知セキュリティレベルが記述された第１のフィールドを有する第１の送信フレームを前記第２の無線通信装置から受信する受信部と、

非暗号化を含む暗号化方法及び暗号化の強さに依存するセキュリティレベルから選定され、前記無線通信グループに割り当てられた基準セキュリティレベルを記憶する第１のメモリ部と、

前記通知セキュリティレベルを前記基準セキュリティレベルと比較して前記第２の無線通信装置との接続拒否或いは接続許可を決定し、決定された接続拒否或いは接続許可が記載される第２のフィールドを有する第２の送信フレームを発生する第１のフレーム発生部と、及び

この第２の送信フレームを前記第２の無線通信装置に向けて送信する送信部と、

を具備することを特徴とする無線通信システムが提供される。

【００２０】

更に、この発明によれば、

通知セキュリティレベルが記述された第１のフィールドを有する第１の送信フレームを通信グループ外から受信し、

非暗号化を含む暗号化方法及び暗号化の強さに依存するセキュリティレベルから選定され、前記無線通信グループに割り当てられた基準セキュリティレベルを記憶し、

前記通知セキュリティレベルを前記基準セキュリティレベルと比較して前記無線通信グループ外の無線通信装置との接続拒否或いは接続許可を決定し、決定された接続拒否或いは接続許可が記載される第２のフィールドを有する第２の送信フレームを発生し、及び

この第２の送信フレームを前記無線通信グループ外の無線通信装置に向けて送信することを特徴とする無線通信方法が提供される。

【００２１】

【発明の実施の形態】

以下、図面を参照して、この発明の無線通信システムに係る実施形態について説明する。

【００２２】

まず、以下の実施形態における無線ＬＡＮシステムで

9

は、複数種類の暗号方式が適用可能であり、その暗号方式の種類が区別され、しかも、暗号化レベルをランク付けしたセキュリティレベルが予め定められている。複数種類の暗号化方式の夫々に異なるレベルがあるとすると、そのある種類の暗号化方式における１つの暗号化レベル毎に、暗号化強度の程度に応じてランクが付され、夫々に対し１つのセキュリティレベルが設定される。従って、同一の暗号化強度を有していても、暗号化方式の種類が異なれば、そのセキュリティレベルとして異なるレベルが与えられる。例えば、セキュリティレベルとして、暗号化の強度の低いものから順に、ｅｎｃ．０、ｅｎｃ．１、ｅｎｃ．２、…、ｅｎｃ．（ｎ－１）のようにｎ個があるものとする。同一強度の暗号化方式が複数種類あっても、その種類毎にランクの異なるセキュリティレベルが設定されるものとする。このように、１つのセキュリティレベルには、１つの種類の暗号化方式が対応し、しかも、同一種類の暗号化方式にあっても暗号化強度の相違により複数のレベルがあるときは、その夫々のレベルに対応しているセキュリティレベルが定められる。

【００２３】

さて、現行のＩＥＥＥ８０２．１１に規定された無線ＬＡＮシステムにおいては、セキュリティレベルの最低レベルは、暗号化なし、即ち、ＷＥＰ（Ｗｉｒｅｄ　Ｅｑｕｉｖａｌｅｎｔ　Ｐｒｉｖａｃｙ）が適応されないレベルが該当する。

【００２４】

現行のＩＥＥＥ８０２．１１に規定に従った無線ＬＡＮ製品では、ＷＥＰが適用される場合にあっても、さらにＷＥＰを６４ビット或いは１２８ビットで構成するというように、２つのレベルがある。そこで、以下の実施形態の例では、複数セキュリティレベルとして、現行のＩＥＥ８０２．１１に規定に従う無線ＬＡＮと同様に、（１）”ＷＥＰなし”、（２）”ＷＥＰありで６４ビットのＷＥＰを利用”、（３）”ＷＥＰありで１２８ビットのＷＥＰを利用”の３つのレベルがある場合を例として説明する。この場合、セキュリティが最も高いのは、（３）”ＷＥＰありで１２８ビットのＷＥＰを利用”であり、これに次いで（４）”ＷＥＰありで６４ビットのＷＥＰを利用”のセキュリティが高くなっている。即ち、”ｅｎｃ．０”が（１）”ＷＥＰなし”に該当し、”ｅｎｃ．１”が（２）”ＷＥＰありで６４ビットのＷＥＰを利用”に該当し、”ｅｎｃ．２”が（３）”ＷＥＰありで１２８ビットのＷＥＰを利用”に該当するものとする。

【００２５】

以下の説明においては、ＷＥＰという１つの種類の暗号化方式のみの場合について説明する。しかし、ＷＥＰ以外の暗号化方式であっても、暗号化方式の種類の相違とセキュリティの強さに応じて複数のレベルを設定するこ

10

とができれば、以下の実施形態の説明と同様にいずれの暗号化方式にあってもこの発明を適用することができる。

【００２６】

以下のこの発明の実施形態では、この発明をＩＥＥ８０２．１１に規定された無線ＬＡＮシステムに適用した場合について説明する。特に、この発明の無線通信装置をＩＥＥ８０２．１１に規定された無線ＬＡＮシステムを構成する基地局或いは端末に適用した場合について説明する。

【００２７】

（第１の実施形態）

まず、この発明の第１の実施形態に無線通信システムとして、複数の端末、例えば、２つの端末（ＷＬ１１～ＷＬ１２）及びこの端末（ＷＬ１１～ＷＬ１２）が無線接続される基地局ＡＰ１が１つのＢＳＳ（ベーシックサービスセット）を構成する通信システムを説明する。

【００２８】

図１は、第１のＢＳＳ（以下、簡単にＢＳＳ１と呼ぶ）を模式的に示したものである。ＢＳＳ１は、アクセスポイントとしての基地局ＡＰ１及び基地局ＡＰ１に接続される複数の端末、例えば、ここでは、２つの無線端末（以下、端末と呼ぶ）ＷＬ１１、ＷＬ１２からなる。

【００２９】

尚、図１には、第１のＢＳＳ１とは異なる第２のＢＳＳ（以下、簡単にＢＳＳ２と呼ぶ）に属する基地局ＡＰ２と、ＢＳＳ１及びＢＳＳ２にも加入していない端末ＷＬ１３も示している。

【００３０】

ＢＳＳ１には、そこで許容する最低のセキュリティレベル（ｅｎｃ＿ｌｏｗ）が設定されている。この実施形態に係る無線通信システムでは、ＢＳＳ１で許容する最低のセキュリティレベル（ｅｎｃ＿ｌｏｗ）は、セキュリティレベル”ｅｎｃ．１”であるとしている。図１には、許容する最低のセキュリティレベル（ｅｎｃ＿ｌｏｗ）がセキュリティレベル”ｅｎｃ．１”である旨をｅｎｃ＿ｌｏｗ＝ｅｎｃ．１と表している。基地局ＡＰ１では、”ｅｎｃ．１”というセキュリティレベル以外にも、セキュリティレベル”ｅｎｃ．１”よりもレベルが高いセキュリティレベル”ｅｎｃ．２”をもサポートしているものとする。従って、ＢＳＳ１で使用可能な最高のセキュリティレベル（ｅｎｃ＿ｈｉｇｈ）は、”ｅｎｃ．２”となる。図１では、最高のセキュリティレベル（ｅｎｃ＿ｈｉｇｈ）が”ｅｎｃ．２”である旨をｅｎｃ＿ｈｉｇｈ＝ｅｎｃ．２と表している。基地局ＡＰ１と、この基地局ＡＰ１に接続される端末或いは基地局とは、”ｅｎｃ．１”以上のセキュリティレベルで通信がされることが予め基地局ＡＰ１に設定されている。同様に、この基地局ＡＰ１を中継して他の装置に通信する為の端末或いは基地局との間は、”ｅｎｃ．１”以上のセ

キュリティレベルで通信がされることが予め基地局ＡＰ１に設定されている。

【００３１】

一方、端末ＷＬ１１の有するセキュリティレベルは、”ｅｎｃ．０”と”ｅｎｃ．１”、端末ＷＬ１２の有するセキュリティレベルは、”ｅｎｃ．０”と”ｅｎｃ．１”と”ｅｎｃ．２”であるとする。

【００３２】

図２は、図１に示された基地局ＡＰ１の回路構成のブロックを示している。尚、以下の説明において、基地局ＡＰ１と基地局ＡＰ２を区別する必要のないとき、或いは、両方に共通する説明の場合には、単に基地局ＡＰと称する。

【００３３】

図２において、受信部１１では、アンテナ２０で端末からの送信信号が受信され、復調及び復号を含む処理によって受信信号が生成される。送信部１２で、アンテナ２０を介して端末へ送信すべき送信信号が生成され、これらの送信信号はアンテナ２０に供給される。

【００３４】

受信部１１からの受信信号は、受信制御部１３に入力され、例えば、ＩＥＥＥ８０２．１１システム（以下の説明において、ＩＥＥＥ８０２．１１システムは、ＩＥＥＥ８０２．１１ａシステム、ＩＥＥＥ８０２．１１ｂシステム及び今後策定されるＩＥＥＥ８０２．１１システムも含むものとする。）に準拠した所定の受信処理などが実施される。この受信制御部１３では、基地局がサポートする複数のセキュリティレベルの夫々に対応する復号化処理を実行し、受信信号は、複合化（ｄｅｃｒｙｐｔ）されて複合化データに変換される。この複合化データは、情報処理部１５に供給されてビデオ、オーディオ、テキスト及び他のタイプのデータに分けられ、必要な処理が施される。

【００３５】

送信制御部１４は、情報処理部１５から供給されたデータを基に、端末へブロードキャスト、或いは、ユニキャストで送信するためのデータを生成する等の、ＩＥＥＥ８０２．１１に準拠した所定の送信処理などを実施する。この送信制御部１４では、基地局がサポートする複数のセキュリティレベルの夫々に対応する暗号化処理を送信すべきデータに施している。送信制御部１４で生成されたデータは、送信部１２を介して送信信号として端末へ送信される。尚、図２に示されるセキュリティテーブル２１については、後に説明する。

【００３６】

図３は、図１に示された端末ＷＬ１１、ＷＬ１２、ＷＬ１３の回路構成の一例を概略的にブロックで示している。尚、以下の説明において、端末ＷＬ１１、ＷＬ１２、ＷＬ１３などを区別する必要のないときは、或いは、全ての端末に共通する説明の場合には、単に端末ＷＬと呼ぶ。

【００３７】

端末ＷＬは、アンテナ１００、アンテナ１００を介して受信信号を受信する受信部１０１、受信部１０１を制御する受信制御部１０５，アンテナ１００を介して送信信号を送信する送信部１０７、この送信部１０７を制御する送信制御部１０６、送信されるデータを生成し、或いは、受信したデータ処理する、例えば、図示しない表示部に表示させる情報処理部１０８及びセキュリティテーブル１１０から構成されている。

【００３８】

情報処理部１０８は、この情報処理部１０８に接続された有線ネットワーク１０９からデータを受け、或いは、ユーザの操作により生成されたデータを基に送信データを作成する。この送信データは、その送信データの送信がユーザによって指示されて送信要求が生ずると、この送信要求を受けて送信データを送信部１０７へ渡す。送信部１０７では、この送信データが規格で定められたディジタルデータに変換され、例えば、ＩＰパケットをＩＥＥＥ８０２．１１で規定するＭＡＣフレーム（ｍｅｄｉｕｍ　ａｃｃｅｓｓ　ｃｏｎｔｒｏｌ　ｆｒａｍｅ）に変換され、ディジタルデータとしてのＭＡＣフレームが所定周波数、例えば、２．４ＧＨｚの無線信号に変換されてアンテナ１００から電波として発信される。

【００３９】

一方、アンテナ１００で受信された受信信号は、受信部１０１でディジタルデータとしてのＭＡＣフレームに変換され、このＭＡＣフレーム中の情報フィールドから受信データが抽出されて情報処理部１０８に送られる。この情報処理部１０８は、受信データをディスプレイに表示する等の処理を行う。尚、情報処理部１０８は、上記以外にも各種情報処理を行うようになっていても良い。また、セキュリティテーブル１１０については、後に説明する。

【００４０】

ＩＥＥＥ８０２．１１で規定されているＭＡＣフレームは、図４に示すように、各種制御情報が納められた最大３０バイトのＭＡＣヘッダー、最大２３１２バイトのデータが収まるデータフィールド（フレームボディ）、そしてデータが正しく送られたのかを調べるためのフレーム・チェック・シーケンス（ＦＣＳ）フィールドで構成されている。ＭＡＣヘッダーには、ＭＡＣフレームを制御する情報が格納されているフレームコントロールフィールド、端末がデータを送れるようにようになるまでの待機時間（ｄｕｒａｔｉｏｎ）或いはＩＥＥＥ８０２．１１においてアソシエーションＩＤと称せられる端末のＩＤが記述されているＤｕｒａｔｉｏｎ／ＩＤｆｉｅｌｄが含まれている。ＢＳＳが基地局ＡＰを備えていれば、このＢＳＳのＩＤとして、基地局ＡＰのＭＡＣアドレスが記述される。また、ＭＡＣヘッダーには、アドレ

13

ス１のフィールドからアドレス４のフィールド及びシーケンスコントロールフィールドが用意されている。データフレームがあるアクセスポイントから他のアクセスポイントに送信される場合には、アドレス１～４は、次のように割り当てられている。即ち、アドレス１のフィールドには、通信システム内の最終的な宛先（Ｄｅｓｔｉｎａｔｉｏｎ　Ａｄｄｒｅｓｓ）のＭＡＣアドレスが記述され、アドレス２のフィールドには、通信システム内における送信元（Ｓｏｕｒｃｅ　Ａｄｄｒｅｓｓ）のＭＡＣアドレスが記述され、アドレス３のフィールドには、当該ＭＡＣフレームを直接送る送信先のＭＡＣアドレスが記述され、アドレス４のフィールドには、当該ＭＡＣフレームを直接送る送信元のＭＡＣアドレスが記述されている。

【００４１】

ＭＡＣフレームのフレームコントロールには、プロトコルのバージョンが記述されているプロトコルバージョンフィールドが設けられ、これに続いてタイプフィールド及びサブタイプフィールドが設けられている。ＭＡＣフレームには、次の３つのタイプがあり、このタイプがフレームコントロールにおけるタイプフィールド（２ビット）に記述されている。また、そのタイプのサブタイプがさらに詳細にサブタイプフィールド（４ビット）に示される。即ち、タイプとして（１）　管理用フレーム、（２）アクセス制御の為の制御用フレーム、（３）データ通信用のデータフレームがある。（１）管理用フレームには、サブタイプとしてビーコン（Ｂｅａｃｏｎ）、オーセンティケーション（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ）のフレーム、アソシエーション（Ａｓｓｏｃｉａｔｉｏｎ）のフレーム、アソシエーションリクエストフレーム、アソシエーション応答フレーム等がある。また、（２）　制御用フレームには、サブタイプとしてＡＣＫ（Ａｃｋｎｏｗｌｅｄｇｍｅｎｔ）、ＲＴＳ（Ｒｅｔｕｒｎ　Ｔｏ　Ｓｅｎｄ）、ＣＴＳ（Ｃｌｅａｒ　Ｔｏ　Ｓｅｎｄ）等のような制御用フレームがある。サブタイプフィールド（４ビット）には、上記のような特定種類のＭＡＣフレーム中のサブタイプがさらに詳細に示されている。

【００４２】

尚、フレームコントロールには、Ｔｏ　ＤＳフィールド（１ビット）及びＦｒｏｍ　ＤＳフィールド（１ビット）が含まれている。これらは、ＭＡＣフレームがデータフレームであるときに利用されるものであって、それ以外の種類のフレーム、例えば、オーセンティケーション、或いは、アソシエーションのフレームでは、常に「０」が書き込まれていて利用されない。ＭＡＣフレームがデータフレームであるとき、データの宛先が有線ＬＡＮ、アクセスポイント或いはＤＳであれば、１のビットがこのＴｏ　ＤＳフィールドに記述され、また、データの送信元が有線ＬＡＮ、アクセスポイント或いはＤＳであれば１のビットがこのＦｒｏｍ　ＤＳフィールドに記述される。フレームコントロールには、リザーブフィールド（ｒｅｓｅｒｖｅｄ　ｆｉｅｌｄ）、ＷＥＰフィールド、オーダーフィールド（ｏｒｄｅｒ　ｆｉｅｌｄ）のような他フィールドが更に用意されている。ユーザによって情報を未だに特に定めがないリザーブフィールドに書き込みをすることができる。図４に示されるように、フレームのタイプ及びサブタイプ或いはフレームのタイプ及びサブタイプのいずれかに従って幾つかのフィールドはリザーブとされている。この発明の実施形態では、後に説明するように、このリザーブフィールドに、暗号化レベルが記述されても良い。この暗号化レベルは、送信データの属性に応じて定められる。機密性が要求されるコンテンツデータであれば、高い暗号化レベルが定められ、このリザーブフィールドにその暗号化レベルが記述される。このリザーブフィールドの暗号化レベルは、アクセスポイントと端末との間でのハンドシェイクする際に利用されても良い。ＷＥＰフィールドには、ＷＥＰが利用される場合には、１のビットがセットされる。

14

【００４３】

再び図１を参照してＢＳＳ１について説明する。

【００４４】

図１に示されるＢＳＳ１では、このＢＳＳ１に予め定められた最低限のセキュリティレベル（ここでは、”ｅｎｃ．１”）で通信が実行されることが予め定められている。即ち、ＢＳＳ１を構成する基地局ＡＰ１と端末ＷＬ１１～ＷＬ１２の夫々とは、セキュリティレベル”ｅｎｃ．１”、或いは、基地局ＡＰ１がサポートしているセキュリティレベルの範囲内で、”ｅｎｃ．１”以上のセキュリティレベルでの通信が実行される。

【００４５】

基地局ＡＰ１及び端末ＷＬ１１～ＷＬ１２の夫々には、記憶部を備え、この記憶部には、セキュリティテーブルが設けられている。基地局ＡＰ１のセキュリティテーブルには、基地局ＡＰ１自身がサポートするセキュリティレベル、このセキュリティレベル中でＢＳＳ１における最低レベルのセキュリティレベルは何れであるか、また、端末ＷＬ１１～ＷＬ１２の夫々がサポートしているセキュリティレベルはどのようなものかが記憶される。また、好ましくは、各セキュリティレベルの暗号化・復号化に必要な情報であって、暗号鍵、或いは、暗号鍵を生成するためのシード情報など（このような暗号化・復号化に必要な情報をここでは、単に暗号パラメータと称する。）もこのセキュリティテーブルに記憶されることが好ましい。また、端末ＷＬ１１～ＷＬ１２の夫々も、セキュリティテーブルが記憶されている記憶部を備え、ＢＳＳ１がサポートするセキュリティレベル中の最低レベルのセキュリティレベル、他の端末のサポートしているセキュリティレベル、さらに、各セキュリティレベル

に対応する暗号パラメータ等がセキュリティテーブルに記憶されている。

【００４６】

図５に示すように、基地局ＡＰ１のセキュリティテーブル２１には、当該基地局ＡＰ１の属するＢＳＳ１においてサポートするセキュリティレベル、ＢＳＳ１に属する全ての端末ＷＬ１１～ＷＬ１２の有するセキュリティレベルが夫々のセキュリティレベルの暗号・複合に必要なデータである暗号パラメータとともに予め登録されている。また、このセキュリティテーブル２１には、基地局ＡＰ１の属するＢＳＳ１における最低レベルのセキュリティレベルとして設定されたセキュリティレベルが識別可能なように登録されている。図５では、セキュリティレベル”ｅｎｃ．１”に対し最低レベルを意味する「○」印が記録されている。

【００４７】

暗号化パラメータは、一例として、ＷＥＰの場合には、ＩＥＥＥ８０２．１１で規定されている秘密鍵（ｋｅｙ１，ｋｅｙ２）及びＩＶ（Ｉｎｉｔｉａｌｉｚａｔｉｏｎ　Ｖｅｃｔｏｒ）等が想定される。尚、以下の説明において、セキュリティレベル及びこのセキュリティレベルに対応する暗号パラメータは、セキュリティ情報と称せられることがある。

【００４８】

図６は、ＢＳＳ１内における端末ＷＬ１１～ＷＬ１２のセキュリティテーブル１１０の登録内容を示している。図６に示すように、端末側のセキュリティテーブルには、ＢＳＳ１内の各端末及び基地局ＡＰ１の有するセキュリティ情報が予め登録されている。基地局ＡＰ１に対応するセキュリティ情報として、図６に示すように、この基地局ＡＰ１の属するＢＳＳ１に予め設定された最低レベルのセキュリティ情報のみが登録されていても良い。また、端末側のセキュリティテーブル１１０は、図５に示した基地局側のセキュリティテーブル２１と全く同じであっても良い。

【００４９】

また、図５及び図６に示したセキュリティテーブルに登録されている基地局ＡＰ１及び各端末のセキュリティレベルは、ＢＳＳ１で予め定められた最低レベル以上のものであれば良い。さらに、各端末に対応するセキュリティ情報については、ＢＳＳ１内において、実際の通信の際に利用されるセキュリティレベルのみが登録されていても良い。即ち、夫々の端末がアクセスポイントに直接リンクされる場合には、アクセスポイントに関するセキュリティ情報、或いは、端末に直接リンクされる場合には、端末に関するセキュリティ情報であって、ＢＳＳ内の端末によってサポートされているセキュリティ情報について、夫々の端末は、そのセキュリティテーブルに保持することができる。

【００５０】

また、図５及び図６に示したセキュリティテーブルは、ＢＳＳ１の初期設定時に設定される。初期設定時には、例えば、図５及び図６に示した形式のテーブルが設定画面として表示され、この画面上に、設定事項を入力するようにしても良い。図５及び図６に示されるテーブルにおいては、ＡＰ１、ＷＬ１，ＷＬ２は、夫々基地局ＡＰ１、端末ＷＬ１，ＷＬ２のＭＡＣアドレスで特定される。

【００５１】

尚、図５及び図６に示すセキュリティテーブルは、初期化の際には、何らの情報も書き込まれていなくとも良い。しかし、アクセスポイントＡＰ１及び端末ＷＬ１、ＷＬ２が図７を参照して後に説明するように非暗号化モードでリンクされれば、セキュリティ情報を書き込むことができる。即ち、アクセスポイントＡＰ１及び端末ＷＬ１、ＷＬ２がアクセスポイントＡＰ１及び端末ＷＬ１、ＷＬ２に関するセキュリティ情報を獲得し、夫々のセキュリティテーブルに書き込み、その後、ＢＳＳ１がアクセスポイントＡＰ１及び端末ＷＬ１、ＷＬ２によって設立され、ＢＳＳ１内での最低のセキュリティレベルが設定されれば良い。

【００５２】

図１に示したＢＳＳ１では、このＢＳＳ１に対し予め設定された最低限のセキュリティレベル”ｅｎｃ．１”以上のセキュリティレベルにて、基地局ＡＰ１及び端末ＷＬ１１～ＷＬ１２間で通信が実行される。

【００５３】

次に、図１に示したＢＳＳ１の基地局ＡＰ１に、このＢＳＳ１に加入していない端末ＷＬ１３が接続される場合について、図７に示すフローチャートを参照して説明する。

【００５４】

端末ＷＬ１３は、基地局ＡＰ１から送信されるＩＥＥＥ８０２．１１に規定されているビーコン（Ｂｅａｃｏｎ）フレームを受信する。ＩＥＥＥ８０２．１１の規定によれば、ビーコンフレームの受信に続いて、次に、オーセンティケーション（ａｕｔｈｅｎｔｉｃａｔｉｏｎ）及びアソシエーション（ａｓｓｏｃｉａｔｉｏｎ）プロトコルが続くが、このオーセンティケーション或いはアソシエーションの為のフレーム中に、基地局ＡＰ１に通知する情報として端末ＷＬ１３のセキュリティレベルが書き込まれる。

【００５５】

図７には、一例としてオーセンティケーションのフレームで端末ＷＬ１３のセキュリティレベルを基地局ＡＰ１に通知する場合の手順を示している。この手順において、端末ＷＬ１３の有するセキュリティレベルは”ｅｎｃ．０”と”ｅｎｃ．１”であると仮定する。

【００５６】

図８（ａ）は、ＩＥＥＥ８０２．１１に規定されている

図４に示されるＭＡＣフレームとしてのオーセンティケーションのフレームにおけるフレームボディのフォーマットを示している。オーセンティケーションフレームには、共通暗号化キーを利用しないオープンシステム及び共通暗号化キーを利用する共通暗号化キーシステムを区別するオーセンティケーションアルゴリズムが記述される。オーセンティケーションアルゴリズム番号には、例えば、オープンシステムでは、”０”が記述され、共通暗号化キーシステムでは、”１”が記述される。オーセンティケーションアルゴリズム番号０で特定されるオープンシステムでは、図８（ｂ）に示すようにオーセンティケーションの要求フレームとしてＡＴＳＮ（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｔｒａｎｓａｃｔｉｏｎ．Ｓｅｑｕｅｎｃｅ Ｎｕｍｂｅｒ）＝１及び＝２のフレームが用意されている。ＡＴＳＮ＝１のオーセンティケーションのフレームは、端末ＷＬから基地局ＡＰ１に送られ、そのステータスコードフィールド（Ｓｔａｔｕｓ Ｃｏｄｅ ｆｉｅｌｄ）は、リザーブとされる。ＡＴＳＮ＝２のオーセンティケーションのフレームは、基地局ＡＰ１から端末ＷＬに送られ、そのステータスコード（Ｓｔａｔｕｓ Ｃｏｄｅ）には、ステータスとして接続拒否或いは接続許可のコードが記載される。オーセンティケーションアルゴリズム番号０で特定されるオープンシステムでは、オーセンティケーションのフレームは、暗号化されるチャレンジテキストが用意されていない。共通暗号化キーシステムでは、オーセンティケーションの要求フレーム（ａｕｔｈｅｎｔｉｃａｔｉｏｎ ｒｅｑｕｅｓｔ）としてＡＴＳＮ（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｔｒａｎｓａｃｔｉｏｎ Ｓｅｑｕｅｎｃｅ Ｎｕｍｂｅｒ）＝１～４のフレームが用意されている。ＡＴＳＮ＝１及びＡＴＳＮ＝３のオーセンティケーションのフレームは、端末ＷＬから基地局ＡＰ１に送られ、そのステータスコードは、リザーブとされる。ＡＴＳＮ＝２及びＡＴＳＮ＝４のオーセンティケーションのフレームは、基地局ＡＰ１から端末ＷＬに送られ、そのステータスコードには、ステータスとして接続拒否或いは接続許可のコードが記載される。共通暗号化システムでは、ＡＴＳＮ＝２及び３のオーセンティケーションのフレームには、暗号化用のチャレンジテキストが用意され、ＡＴＳＮ＝３のオーセンティケーションのフレームは暗号化されている。これに対して、ＡＴＳＮ＝１及び４のオーセンティケーションのフレームには、暗号化用のチャレンジテキストが用意されていない。

【００５７】

ＡＴＳＮ＝１で特定されるオーセンティケーションのフレームは、接続要求を発する側から送信される。この要求フレームでは、そのステータスコードフィールドは、リザーブとされ現在未使用である。従って、このステータスコードフィールドに、接続要求を発する側のセキュリティレベル”ｅｎｃ．１”或いは”ｅｎｃ．２”を書き込むことができる。以下の実施形態の説明では、Ｓｔａｔｕｓｃｏｄｅ ｆｉｅｌｄに、接続要求を発する側のセキュリティレベル”ｅｎｃ．１”或いは”ｅｎｃ．２”が書き込まれているものとする。このＡＴＳＮ＝１のオーセンティケーションのフレームには、端末ＷＬ１３の送信部１０７で基地局ＡＰ１との通信で利用したいセキュリティレベル（例えば、”ｅｎｃ．　１”）を示すデータがそのステータスコードの項に書き込まれ、このＡＴＳＮ＝１のオーセンティケーションのフレームが図７のステップＳ２に示すように、基地局ＡＰ１に送信される。尚、このセキュリティレベルは、図４に示したＭＡＣフレーム中のいずれかのリザーブフィールドに書き込まれても良い。

【００５８】

ＡＴＳＮ＝１のオーセンティケーションのフレームを受信した基地局ＡＰ１の処理動作について説明する。既に記載したように、基地局ＡＰ１から常に発せられているビーコンフレームがステップＳ１に示すように端末ＷＬ１３によって検出される。この検出の後に、端末ＷＬ１３の送信制御部１０６は、ＡＴＳＮ＝１のオーセンティケーションフレームを用意し、セキュリティテーブル１１０を参照してそのフレームの所定箇所、例えば、フレームボディ中のステータスコードにセキュリティレベル”ｅｎｃ．１”或いは”ｅｎｃ．２”を書き込む。セキュリティレベルが書き込まれたオーセンティケーションフレームは、端末ＷＬ１３の送信制御部１０６によって検出したビーコンフレームに対応する基地局ＡＰ１を送り先としてアドレス２に指定して、ステップＳ２に示すように基地局ＡＰ１に送信される。基地局ＡＰ１は、オーセンティケーションフレームを受信し、基地局ＡＰ１の受信制御部１３は、受信したＡＴＳＮ＝１のオーセンティケーションフレームの所定箇所、例えば、フレームボディ中のステータスコードに書き込まれている端末ＷＬ１３のセキュリティレベル”ｅｎｃ．１”或いは”ｅｎｃ．２”を取り出し、基地局ＡＰ１のセキュリティテーブル２１に登録されているＢＳＳ１の最低レベルのセキュリティレベル”ｅｎｃ＿ｌｏｗ”と比較する。ステップＳ３に示すように端末ＷＬ１３から通知されたこの端末ＷＬ１３のセキュリティレベル”ｅｎｃ．１”或いは”ｅｎｃ．２”が、基地局ＡＰ１がサポートしているセキュリティレベル”ｅｎｃ．１”或いは”ｅｎｃ．２”であり、しかも、ＢＳＳ１内における最低レベルのセキュリティレベル”ｅｎｃ＿ｌｏｗ”以上のときには、端末ＷＬ１３の接続を許可すると判断する。端末ＷＬ１３のセキュリティレベルが、基地局ＡＰ１がサポートしているセキュリティレベルでない場合、或いは、基地局ＡＰ１がサポートしているセキュリティレベルであるが、ＢＳＳ１における最低レベル”ｅｎｃ＿ｌｏｗ”のセキュリティレベル未満のときは端末ＷＬ１３の接続を拒否すると判断する。

19

【００５９】
ステップＳ３において、基地局ＡＰ１が端末ＷＬ１３の接続を拒否する場合は、ＩＥＥＥ８０２．１１に規定に従い、ＡＴＳＮ＝２のオーセンティケーションフレームが送信制御部１２によって用意され、そのステータスコードに接続が失敗である旨のコードが書き込まれ、ステップＳ４に示すように端末ＷＬ１３にＡＴＳＮ＝２のオーセンティケーションフレームが返信される。端末ＷＬ１３は、ステップＳ５に示されるように接続を拒否する記述がされたＡＴＳＮ＝２のオーセンティケーションフレームの受信がＮ回目かを判断する。このＮ回は、端末側のセキュリティテーブル１１０に書き込まれているセキュリティレベルの数（＝Ｎ個）に相当している。当初、基地局ＡＰ１がサポートしているセキュリティレベルが低いレベルとして端末ＷＬ１３は、この低いレベルのセキュリティレベルを基地局に通知し、拒否されるとそのセキュリティレベルを上げ、ステップＳ２に示すように上げられたセキュリティレベルが通知される。端末側のセキュリティテーブル１１０がサポートしているＮ個のセキュリティレベルを通知して、ステップＳ５に示すようにＮ回に亘ってＡＴＳＮ＝２のオーセンティケーションフレームを端末ＷＬ１３が受信する場合には、基地局ＡＰ１から接続を拒否されたと判断して、この段階でステップＳ１５に示すように接続手続きが中断される。

【００６０】
一方、端末ＷＬ１３の接続を許可する場合は、基地局ＡＰ１は、端末ＷＬ１３から通知されたセキュリティレベルに対応する暗号パラメータを端末ＷＬ１３と共有すべく、ステップＳ６に示すようにＩＥＥＥ８０２．１１に規定に従い、チャンレンジテキストを送信するＡＴＳＮ＝２のオーセンティケーションフレームを用意し、このオーセンティケーションフレームのステータスコードに、ＡＴＳＮ＝１のオーセンティケーションフレームの受信が成功である旨のコードを書き込み、ステップＳ６に示すように端末ＷＬ１３に返信する。

【００６１】
端末ＷＬ１３では、ＡＴＳＮ＝２のオーセンティケーションフレームを受信すると、基地局ＡＰ１と端末ＷＬ１３との間のセキュリティレベル、例えば、セキュリティレベル”ｅｎｃ．１”が確定される。また、端末ＷＬ１３は、セキュリティレベルに対応する暗号パラメータとして、ユーザによって予め取得したＩＶや秘密鍵を用いて、ＩＥＥＥ８０２．１１の規定に従い、チャレンジテキストなどを含むフレームボディを、ステップＳ７に示すように端末ＷＬ１３の有するＷＥＰ機能を用いて暗号化する。更に、端末ＷＬ１３は、ＡＴＳＮ＝３のオーセンティケーションフレームを用意し、そのフレームボディにＡＴＳＮ＝２のオーセンティケーションフレームからチャレンジテキストをコピーする。この端末ＷＬ１３

20

は、フレームを暗号化してステップＳ８に示すように基地局ＡＰ１に送信する。

【００６２】
ＡＴＳＮ＝３のオーセンティケーションフレームを受信した基地局ＡＰ１では、同じくＩＥＥＥ８０２．１１に規定に従い、端末ＷＬ１３とで共有されている基地局ＡＰ１が有する秘密鍵で、ステップＳ９に示すように受信したＡＴＳＮ＝３のオーセンティケーションフレームを復号して格納された暗号化チャレンジテキストを取り出すこととなる。この複合化されたチャレンジテキストは、送信されたチャレンジテキストと比較され、ステップＳ１０に示すようにその比較結果を基に暗号化・複合化が検証される。

【００６３】
検証結果が「失敗」であれば、同じくＩＥＥＥ８０２．１１に規定に従い、その旨を通知するＡＴＳＮ＝４のオーセンティケーションフレームが用意され、そのステータスコードに、検証結果が「失敗」である旨のコードが書き込まれ、ステップＳ１１に示すようにＡＴＳＮ＝４のオーセンティケーションフレームが端末ＷＬ１３に返信される。検証結果の「失敗」は、暗号化方式が基地局ＡＰ１と端末ＷＬ１３とで相違していることを意味している。従って、ステップＳ１４に示すようにＡＴＳＮ＝４のオーセンティケーションフレームがＭ回以内であることが確認されて端末ＷＬ１３における暗号化方式が変更されてステップＳ２に戻され、ステップＳ２からステップＳ１０が繰り返される。ここで、Ｍ回は、端末ＷＬ１３が用意している暗号化方式の個数に対応し、端末ＷＬ１３は、Ｍ回ＡＴＳＮ＝４のオーセンティケーションフレームを受信することができる。このように端末ＷＬ１３がＭ回ＡＴＳＮ＝４のオーセンティケーションフレームを受けても暗号化方式が一致しない場合には、端末ＷＬ１３は、基地局ＡＰ１との接続が拒否された判断される。従って、端末側では、基地局ＡＰ１が提供する暗号化方式を準備していないとして、ステップＳ１５に示すように接続手続きが終了される。

【００６４】
一方、ステップＳ１０における検証結果が「成功」であれば、基地局ＡＰ１は、ステップＳ１２に示すように同じくＩＥＥＥ８０２．１１に規定に従い、その旨を通知するＡＴＳＮ＝４のオーセンティケーションフレームを端末ＷＬ１３に送信する。端末ＷＬ１３では、このフレームを受信すると、ステップＳ１２に示すように次の手順であるＩＥＥＥ８０２．１１に規定されたアソシエーションを開始する。即ち、端末ＷＬ１３は、ステップＳ１３に示すようなアソシエーションリクエストフレームを基地局ＡＰ１に送り、このリクエストに応答して基地局ＡＰ１は、アソシエーションリスポンス端末ＷＬ１３に返すようなＩＥＥＥ８０２．１１に規定に従った処理動作が実行される。アソシエーションが正常に終了した

後、端末ＷＬ１３と基地局ＡＰ１との間では、データフレームが送受信される。その送受信されるデータフレームは、上記手順によって予め定められた暗号化、例えば、”ｅｎｃ．１＝ｅｎｃ．ｌｏｗ”のセキュリティレベルに相当する６４ビットのＷＥＰ機能により暗号化されている。

【００６５】

尚、端末ＷＬ１３及び基地局ＡＰ１では、その端末ＷＬ１３及び基地局ＡＰ１間の通信のセキュリティレベル及び暗号パラメータが確定した時点で、互いのセキュリティ情報がそのセキュリティテーブル２１，１１０に登録される。即ち、端末ＷＬ１３では、図７に示すステップＳ７で暗号パラメータを取得した後に、基地局ＡＰ１のセキュリティ情報がセキュリティテーブル１１０に登録される。また、基地局ＡＰ１では、図７のステップＳ１０で検証が成功した後に、端末ＷＬ１３のセキュリティ情報がそのセキュリティテーブル２１に登録される。即ち、図４に示されるＭＡＣフレーム中の端末ＷＬ１３のアドレスを示す適切なアドレスフィールドを選択することによってこのアドレスとの関係でセキュリティ情報がアクセスポイントＡＰ１のセキュリティテーブル２１に登録される。基地局ＡＰ１のセキュリティテーブルには、図１０に示すように、「接続先」が端末ＷＬ１３であるセキュリティ情報が新たに登録される。端末ＷＬ１３のセキュリティテーブルにも、同様にして「接続先」が基地局ＡＰ１であるセキュリティ情報が新たに登録される。即ち、図４に示されるＭＡＣフレーム中の基地局ＡＰ１のアドレス１を示す適切なアドレスフィールドを選択することによってこのアドレスとの関係でセキュリティ情報が端末ＷＬ１３のセキュリティテーブル１１０に登録される。この新たに追加された端末ＷＬ１３におけるセキュリティ情報のセキュリティレベルは、端末ＷＬ１３が図７のステップＳ２で要求してきたセキュリティレベルに相当している。

【００６６】

また、端末側のセキュリティテーブルに、基地局のセキュリティ情報が登録されていれば、端末は、その基地局の最低レベル以上のセキュリティレベルを予め選択することができ、その結果、ステップＳ３で、当該基地局から接続を拒絶されることがない。ここで、基地局のセキュリティ情報は、少なくとも当該基地局の属するＢＳＳに予め定められた最低レベル以上のセキュリティレベルを有する。換言すれば、端末が基地局に再接続する際に、基地局に端末自身がサポートしているセキュリティレベルの中から基地局で定められた最低レベル以上のセキュリティレベルを選択して図７におけるステップＳ２に示すようにこのセキュリティレベルを基地局に通知すれば良い。

【００６７】

また、基地局ＡＰのセキュリティテーブルに、端末ＷＬ

に関するセキュリティ情報として少なくとも当該基地局の属するＢＳＳに予め定められた最低レベルｅｎｃ＿ｌｏｗ以上のセキュリティレベルのセキュリティ情報が登録されていることが好ましい。この登録において、基地局の属するＢＳＳに関しては、図４に示すＭＡＣフレームにおける適切なアドレスフィールドに記載されたアドレスでＢＳＳが特定され、このアドレス及びセキュリティレベルがセキュリティテーブルに記述される。このようなＢＳＳに関する登録があれば、基地局から当該端末へのユニキャスト通信に用いるセキュリティレベルを、当該最低レベル以上で、しかも、当該端末がサポートすることができるセキュリティレベルを予め選択することできる。また、基地局ＡＰの属するＢＳＳ内の端末ＷＬへのマルチキャスト通信、ブロードキャスト通信におけるセキュリティレベルも、当該最低レベルｅｎｃ＿ｌｏｗ以上で、しかも、それを受信すべき全ての端末にてサポートされているセキュリティレベルのものを予め選択することができる。即ち、図７のステップＳ５に示すように、基地局ＡＰ１から接続を拒否されたときには、先に通知したセキュリティレベルとは異なる、好ましくは、より高いレベルのセキュリティレベルを通知して、再度接続の要求することができる。端末ＷＬ１３が有するセキュリティレベルを１つずつ通知しながら、最大所定回数Ｍだけ接続要求が可能となる。

【００６８】

基地局ＡＰ１は、接続要求元の端末ＷＬ１３に対し、ＢＳＳ１に予め設定された最低レベルのセキュリティレベルｅｎｃ＿ｌｏｗ、或いは、基地局ＡＰ１がサポートしている最低レベルｅｎｃ＿ｌｏｗ以上のセキュリティレベルの全てを通知するようにしても良い。この通知は、ＩＥＥＥ８０２．１１に規定されているＭＡＣフレームの管理用フレーム、制御用フレームのうち現在未使用のフレームを用いて通知するようにしても良い。例えば、管理用フレームでは、サブタイプが「０１１０」～「０１１１」などのフレーム、制御用フレームでは、サブタイプが「００００」～「１００１」などのフレームが相当する。図７に示されるステップＳ４において、基地局ＡＰ１が端末の接続を拒否した場合において、ＡＴＳＮ＝２のオーセンティケーションフレームを送信した後に、この未使用のフレームを送信して最低レベルｅｎｃ＿ｌｏｗ以上のセキュリティレベルの全てを端末ＷＬ１３に通知するようにしても良い。また、ステップＳ４或いはステップＳ６おいて、ＡＴＳＮ＝２のオーセンティケーションフレームを送信する前に未使用のフレームを送信して最低レベルｅｎｃ＿ｌｏｗ以上のセキュリティレベルの全てを端末ＷＬ１３に通知しても良い。更に、オーセンティケーション或いはアソシエーションの処理の間、或いは、データフレームの送受信が開始する前等、適当なときを見計らってアクセスポイントＡＰ１が未使用のフレームを送信して最低レベルｅｎｃ＿ｌｏｗ

以上のセキュリティレベルの全てを端末ＷＬ１３に通知するようにしても良い。

【００６９】

ＩＥＥＥ８０２．１１に規定されているＭＡＣフレームのアソシエーションのフレームには、図９（ａ）、図９（ｂ）及び図９（ｃ）に示すように、そのフレームボディの「キャパビリティー情報（Ｃａｐａｂｉｌｉｔｙ ｉｎｆｏｒｍａｔｉｏｎ）」内に未使用領域としてリザーブフィールドが設けられている。この未使用領域を利用して、基地局ＡＰ１は、接続要求元の端末ＷＬ１３にＢＳＳ１の最低レベルのセキュリティレベルｅｎｃ＿ｌｏｗ、或いは、基地局ＡＰ１がサポートしている当該最低レベルｅｎｃ＿ｌｏｗ以上のセキュリティレベルの全てを端末ＷＬ１３に通知するようにしても良い。

【００７０】

このように、上記第１の実施形態では、基地局ＡＰ１に、ＢＳＳ１内に属する端末ＷＬ１１，Ｗｌ１２以外のＢＳＳ１内に属さない端末ＷＬ１３が接続しようとする場合、まず、

（１）この端末ＷＬ１３は、基地局ＡＰ１へ、端末ＷＬ１３自身のセキュリティレベルを通知する。図７に示されるフローでは、この通知は、オーセンティケーションのフレームを利用している。

【００７１】

（２）基地局ＡＰ１では、この端末ＷＬ１３から通知されるセキュリティレベルが基地局ＡＰ１でサポートしているセキュリティレベルであり、しかも、ＢＳＳ１に予め定められた最低レベルｅｎｃ＿ｌｏｗのセキュリティレベル以上であるときには、端末ＷＬ１３の接続を許可して、接続のための処理動作を続行する。しかし、端末ＷＬ１３から通知されるセキュリティレベルがＢＳＳ１に予め定められた最低レベルのセキュリティレベルに満たないときには、端末ＷＬ１３の接続を拒否する。

【００７２】

（３）端末ＷＬ１３からの接続を許可する場合には、必要に応じて、暗号化・復号化のための情報、即ち、暗号パラメータを共有するための認識処理が実行される。

【００７３】

このように、上記第１の実施形態によれば、ＢＳＳといった、無線ＬＡＮの基本グループ毎に、夫々のグループで予め定められた暗号化による最低限のセキュリティレベルを確保した無線通信が実現される。

【００７４】

好ましくは、上記（１）の場合、端末ＷＬ１３は、端末ＷＬ１３自身がサポートするセキュリティレベルのうち、最高レベルｅｎｃ＿ｈｉｇｈのセキュリティレベルを基地局ＡＰ１に通知されれば、基地局ＡＰ１が端末ＷＬ１３の接続を拒否する機会が少なくなる。また、最高レベルｅｎｃ＿ｈｉｇｈのセキュリティレベルを基地局ＡＰ１に通知すれば、１回の接続要求で、当該基地局ＡＰ１との接続の可否が判断でき、結果として、無駄なトラヒックを削減することができる。

【００７５】

また、ＢＳＳ１内の基地局或いは各端末は、夫々ＢＳＳ１内の基地局或いは端末と通信する際に利用するＢＳＳ１に予め定められた最低レベルｅｎｃ＿ｌｏｗ以上のセキュリティレベルのセキュリティ情報をセキュリティテーブルに登録することが好ましい。基地局或いは各端末は、このセキュリティテーブルを参照して、アドレスで特定される所望の端末や基地局に接続要求する際に通知するセキュリティレベルとして接続を拒否されない最低限のセキュリティレベルを予め選択することができる。

【００７６】

上記第１の実施形態では、ステップＳ２において、端末ＷＬ１３が基地局ＡＰ１との通信で利用することを希望する１つのセキュリティレベルのみを基地局ＡＰ１に通知しているが、この場合に限られるものではないことは明らかである。端末ＷＬ１３自身が有する全て、或いは、全てでなくとも複数のセキュリティレベルが端末ＷＬ１３から基地局ＡＰ１に通知されても良い。また、端末ＷＬ１３がサポートするセキュリティレベルのうち、最高レベルのセキュリティレベルｅｎｃ＿ｈｉｇｈのみが端末ＷＬ１３から基地局ＡＰ１に通知されても良い。

【００７７】

ステップＳ２において、端末ＷＬ１３自身が有する全て、或いは、全てでなくとも複数のセキュリティレベルを通知する場合における基地局ＡＰ１の処理動作について説明する。

【００７８】

図７に示すステップＳ２において、端末ＷＬ１３自身が有する複数のセキュリティレベルが基地局に送信される。基地局ＡＰ１では、ステップＳ３では、このセキュリティレベルの中に、ＢＳＳ１における最低レベルに相当するセキュリティレベルｅｎｃ＿ｌｏｗ以上のセキュリティレベルであって、しかも自装置がサポートしているセキュリティレベルが含まれているかを判断する。基地局ＡＰ１は、サポートしているセキュリティレベルが含まれているときは、端末ＷＬ１３の接続を許可すると判断する。また、基地局ＡＰ１は、サポートしているセキュリティレベルが含まれていないときは端末ＷＬ１３の接続を拒否すると判断する。端末ＷＬ１３の接続を拒否する場合は、ステップＳ４へ進む。端末ＷＬ１３の接続を許可するときは、基地局ＡＰ１は、次に、端末ＷＬ１３と基地局ＡＰ１とが共にサポートしているセキュリティレベルのうち、ＢＳＳ１における最低レベルｅｎｃ＿ｌｏｗ以上のセキュリティレベルを選択する。基地局ＡＰ１は、ＢＳＳ１における最低レベルｅｎｃ＿ｌｏｗ以上のセキュリティレベルが複数存在するときは、その中の１つを選択する。この選択に関しては、その中で最低のもの、或いは最高のもの、その他の各種選択基準が

25

あるが、そのいずれであってもその中の１つを選択すれば良い。基地局ＡＰ１は、選択した１つのセキュリティレベルを端末ＷＬ１３との間の通信に用いるセキュリティレベルとする。例えば、端末ＷＬ１３から通知されたセキュリティレベルが”ｅｎｃ．　０”と”ｅｎｃ．１”であるとすると、端末ＷＬ１３の基地局ＡＰ１への接続は許可され、端末ＷＬ１３と基地局ＡＰ１との間の通信のセキュリティレベルは”ｅｎｃ．　１”と選択される。

【００７９】

この選択されたセキュリティレベルを端末ＷＬ１３へ通知する必要がある場合には、例えば、図７のステップＳ６にて、ＡＴＳＮ＝２のオーセンティケーションフレームを送信する前などに、前述のＩＥＥＥ８０２．１１に規定されているＭＡＣフレームの管理用フレーム、制御用フレームのうち現在未使用のフレームなどを用いても良い。

【００８０】

端末ＷＬ１３では、選択されたセキュリティレベルの通知を受けて、その後の処理の準備を行うことができる。

【００８１】

ＢＳＳ１内では、ＢＳＳ１に予め定められた最低レベルｅｎｃ＿ｌｏｗ以上のセキュリティレベルであるなら、必ずしも同一のセキュリティレベルで通信する必要はない。

【００８２】

また、ＢＳＳ１内では、接続相手に応じて異なるセキュリティレベルで通信するようにしても良い。即ち、ここでは、基地局ＡＰ１は、ＢＳＳ１に予め定められた最低レベルｅｎｃ＿ｌｏｗ以上のセキュリティレベルであるなら、どのセキュリティレベルでどの端末と通信することに関し特に限定はない。基地局ＡＰ１が端末毎に異なるセキュリティレベルで通信することにより、無線通信の秘匿性を向上することができる。

【００８３】

図７は、ＢＳＳ１に加入していない端末ＷＬ１３と基地局ＡＰ１との間の接続時の動作として説明したが、上記の説明の端末ＷＬ１３をＢＳＳ１に加入している端末ＷＬ１１～ＷＬ１２の夫々に置き換えても良い。端末ＷＬ１１～ＷＬ１２の夫々が、基地局ＡＰ１と接続しようとするときも、図７に示した手順に従えば、図７のステップＳ２で、その都度異なるセキュリティレベルを通知して、接続の度に、その目的に応じたセキュリティレベルを変更することができる。この場合、各端末のセキュリティテーブルには、ＢＳＳ１の最低レベルのセキュリティレベルが登録されているので、各端末がサポートするセキュリティレベルのうち、この最低レベル以上のセキュリティレベルが選択されて、それがステップＳ２で通知される。また、セキュリティレベルを変更しなくとも、その後のオーセンティケーションの際に、暗号パラメータ（ＷＥＰの場合、秘密鍵やＩＶなど）を変更することもできる。

26

【００８４】

同様に、図７の説明の端末から基地局への接続要求の際の手順は、互いに異なるＢＳＳに属する、基地局から基地局へ接続要求の際の手順としても適用可能である。即ち、図７の説明の端末ＷＬ１３を基地局ＡＰ１、基地局ＡＰ２をＢＳＳ１とは異なる他のＢＳＳに属する基地局、例えば、ここではＢＳＳ２の基地局ＡＰ２に置き換えることができる。このように、第１の実施形態によれば、基地局間の通信、即ち、ＤＳ通信においても、夫々の最低限のセキュリティレベル以上で通信が実現される。

【００８５】

ＢＳＳ１内の端末、例えば、端末ＷＬ１１が同じＢＳＳ１内の他の端末、例えば、端末ＷＬ１２、と通信する際には、必ず、基地局ＡＰ１を介して基地局ＡＰ１に接続して通信しても良く、基地局ＡＰ１を介さず、端末間で直接通信しても良い。

【００８６】

端末ＷＬ１１～ＷＬ１２、基地局ＡＰ１が、夫々のセキュリティテーブルに登録されている相手に接続しようとする場合、セキュリティレベル及び暗号パラメータを送受信するためのオーセンティケーションなどを省略しても良い。接続要求を受けた側では、そのフレームの送信元が自身のセキュリティテーブルに登録されているものであれば、そのセキュリティテーブルを参照して、ＢＳＳ１内で予め定められた最低レベル以上のセキュリティレベルで要求元と通信すれば良い。

【００８７】

基地局ＡＰ１及び端末ＷＬ１１～ＷＬ１２の夫々のセキュリティテーブルに、接続相手毎に、過去にその間の通信で用いたセキュリティレベルのセキュリティ情報のみが登録されても良い。この登録されているセキュリティ情報は、ＢＳＳ１における最低レベルｅｎｃ＿ｌｏｗ以上のセキュリティレベルに相当する。

【００８８】

初期設定時においては、ＢＳＳ１内の基地局ＡＰ１及び端末ＷＬ１１～ＷＬ１２のセキュリティテーブルは、全て同一の内容が記載され、図５に示すような、ＢＳＳ１を構成する各装置に対し、その夫々がサポートする全てのセキュリティレベルのセキュリティ情報及びＢＳＳ１に最低レベルとして設定されたセキュリティレベルとが登録されていても良い。

【００８９】

また、ＢＳＳ１内では、基地局ＡＰ１及び端末ＷＬ１１～１２もＢＳＳ１で許容する最低のセキュリティレベルである”ｅｎｃ．　１”はサポートする。従って、端末ＷＬ１１～ＷＬ１２のいずれかがデータフレームなどをＢＳＳ１内でマルチキャスト、ブロードキャストすると

きには、そのフレームのフレームボディは許容する最低のセキュリティレベルで暗号化されるものとする。これにより、ＢＳＳ１としては、許容する最低のセキュリティレベルを確保できる。

【００９０】

また、上記第１の実施形態では、接続要求元のサポートしているセキュリティレベルのチェックと、暗号パラメータを接続要求元と接続要求先とで共有するための認識処理とをＩＥＥＥ８０２．１１に規定されているオーセンティケーション時にまとめて行っている。しかし、この２つの処理を分けて、前者をＩＥＥＥ８０２．１１に規定されているアソシエーション時に処理を実行することもできる。また、先にアソシエーションを行なって、次に、オーセンティケーションを行う場合も考えられる。この場合において、上記２つの処理をオーセンティケーション時にまとめて行ってもよいし、アソシエーション時とオーセンティケーション時とに分けて行うようにしても良い。しかし、上記２つの処理を分ける場合、好ましくは、セキュリティレベルのチェックを暗号パラメータを共有するための認識処理に先だって行った方が、セキュリティを確保する上で好ましい。

【００９１】

（第２の実施形態）

最低限のセキュリティレベルが予め定められた図１に示されるようなＢＳＳ１の基地局が当該ＢＳＳ１で定められた最低限のセキュリティレベルをブロードキャストする第２の実施に係る通信システムについて説明する。この説明においては、第２の実施形態に係る通信システムにおいて、第１の実施形態と同一の説明については、省略し、その異なる点について図１２を参照して説明する。

【００９２】

第２の実施形態に係る通信システムにおいては、ＩＥＥＥ８０２．１１に規定されたビーコンフレームに当該ＢＳＳの最低限のセキュリティレベルが書き込まれ、このビーコンフレームが送信される

図１１は、ＩＥＥＥ８０２．１１に規定されているＭＡＣフレームの構造を有するビーコンフレームのフレームボディのフォーマットを示している。このビーコンフレームの「キャパビリティー情報（Ｃａｐａｂｉｌｉｔｙ　ｉｎｆｏｒｍａｔｉｏｎ）」内には、未使用領域としてリザーブフィールドが設けられている。基地局ＡＰ１は、ＢＳＳ１の最低レベルのセキュリティレベル或いは、基地局ＡＰ１がサポートしている当該最低レベル以上のセキュリティレベル全て、或いは全てでなくとも複数のセキュリティレベルをこのリザーブフィールドに書き込み、そのセキュリティレベルを端末ＷＬに通知する。

【００９３】

基地局ＡＰ１の送信制御部１４は、ビーコンフレームに

ＢＳＳ１の最低レベルのセキュリティレベル或いは、基地局ＡＰ１がサポートしている当該最低レベル以上のセキュリティレベル全て、或いは、全てでなくとも複数のセキュリティレベルを書き込み、ブロードキャストする。図１２のステップＳ２１に示すように、このビーコンフレームを端末が受信する。ビーコンフレームは、ＢＳＳ１に加入していない端末、例えば、図１に示す端末ＷＬ１３も受信することができる。

【００９４】

端末ＷＬ１３の受信部１０１では、ステップＳ２２に示すように受信したビーコンフレームに書き込まれたＢＳＳ１の最低レベルのセキュリティレベルを取り出し、ステップＳ２３に示すように端末ＷＬ１３がサポートしているセキュリティレベルに、ＢＳＳ１の最低レベル以上のものがあるか否かチェックする。ここで、端末ＷＬ１３がサポートしている全てのセキュリティレベルは、予め端末ＷＬ１３のセキュリティテーブルに登録されていても良い。端末ＷＬ１３のセキュリティレベルに、ＢＳＳ１の最低レベル以上のものがないときは、基地局ＡＰ１との接続は中止してその接続処理を終了する。

【００９５】

ここでは、ＢＳＳ１の最低レベルのセキュリティレベルは”ｅｎｃ．１”であり、端末ＷＬ１３は、”ｅｎｃ．０”と”ｅｎｃ．１”をサポートしているので、端末ＷＬ１３は、基地局ＡＰ１と接続可能である。端末ＷＬ１３のセキュリティレベルには、ＢＳＳ１の最低レベル以上のものがあるので、端末ＷＬ１３は、この”ｅｎｃ．１”というセキュリティレベルを選択して、基地局ＡＰ１への接続要求を開始する。即ち、図７のステップＳ２へ進み、選択したセキュリティレベルを通知し、以下、第１の実施形態の説明と同様の動作を行う。

【００９６】

但し、この場合、端末ＷＬ側からは、必ず、最低レベル以上のセキュリティレベルが通知されることが期待できるので、基地局ＡＰ１では、図７のステップＳ３を省略しても良い。また、端末ＷＬ１３は、ステップＳ２において、端末ＷＬ１３自体が有するセキュリティレベルのうち、ビーコンフレームにて通知されたＢＳＳ１の最低レベル以上のセキュリティレベルを選択して（このようなセキュリティレベルが複数あるときは、それら全て、或いは、そのうちの所望のいくつか、或いは、そのうちの１つを選択して、例えば、セキュリティレベルが最高のもの、或いは最低のもの、或いは所望のものを選択しても良い。）基地局ＡＰ１へ通知すれば良い。

【００９７】

このように、最低限のセキュリティレベルが予め定められたＢＳＳ１の基地局ＡＰ１が、当該ＢＳＳの最低限のセキュリティレベルをブロードキャストすることにより、端末ＷＬ１３は、自身がサポートするセキュリティレベルで接続可能な相手を予め選択してから接続を開始

するので、不要なトラヒックを削減することができる。

【００９８】

また、端末ＷＬ１３が基地局ＡＰ１に対し、ｐｒｏｂｅの要求フレーム（ｐｒｏｂｅ　ｒｅｑｕｅｓｔ）を送信し、それに対し基地局ＡＰ１がｐｒｏｂｅの応答フレーム（ｐｒｏｂｅ　ｒｅｓｐｏｎｓｅ）でセキュリティレベルを通知することもできる。

【００９９】

（第３の実施形態）

上記第１の実施形態では、ＩＥＥＥ８０２．１１に規定されたオーセンティケーションとアソシエーションとを、この順で実施する場合について説明したが、先にアソシエーションを行ってからオーセンティケーションを実施することも想定される。第３の実施形態では、この場合について、図１に示したＢＳＳ１の場合を例にとし、図１３に示したフローチャートを参照して説明する。

【０１００】

ここでも、第１の実施形態と同様、ＢＳＳ１の基地局ＡＰ１に、ＢＳＳ１に加入していない端末ＷＬ１３が接続を要求する場合について説明し、第１の実施形態と異なる部分についてのみ説明する。

【０１０１】

端末ＷＬ１３は、ステップＳ３１に示すように基地局ＡＰ１から送信されるビーコンフレームを受信し、その後、基地局ＡＰ１に接続すべく、ステップＳ３２に示すようにアソシエーションの要求フレームを基地局ＡＰ１に送信する。

【０１０２】

前述したように、ＩＥＥＥ８０２．１１に規定されているＭＡＣフレームのアソシエーションのフレームには、図９（ａ）、図９（ｂ）及び図９（ｃ）に示すように、そのフレームボディの「キャパビリティー情報（Ｃａｐａｂｉｌｉｔｙｉｎｆｏｒｍａｔｉｏｎ）」内に未使用領域、即ち、リザーブフィールドが用意されている。端末ＷＬ１３の送信部１０７は、このリザーブフィールドに端末ＷＬ１３のサポートしているセキュリティレベルのうち少なくとも所望の１つをこのリザーブフィールドに書き込み、ステップＳ３２に示すよう基地局ＡＰ１に送信する。例えば、ここでは、端末ＷＬ１３の送信部１０７では、自身のもつ全てのセキュリティレベル（”ｅｎｃ．０””ｅｎｃ．１”）のうちの１つの”ｅｎｃ．１”を示すデータをリザーブフィールドに書き込み、基地局ＡＰ１に送信するものとする。

【０１０３】

これを受信した基地局ＡＰ１の処理動作は、第１の実施形態と同様である。即ち、基地局ＡＰ１の受信制御部１３は、受信したアソシエーションの要求フレーム（Ａｓｓｏｃｉａｔｉｏｎ　Ｒｅｑｕｅｓｔ）に書き込まれている端末ＷＬ１３のセキュリティレベルを取出し、この

セキュリティレベルを基地局ＡＰ１のセキュリティテーブル２１に登録されているＢＳＳ１の最低レベルのセキュリティレベルと比較する。端末ＷＬ１３から通知された、この端末ＷＬ１３のセキュリティレベルが基地局ＡＰ１のサポートしているセキュリティレベルであり、しかも、ＢＳＳ１における最低レベルのセキュリティレベル以上のときには、ステップＳ３３に示すように端末ＷＬ１３の接続を許可すると判断する。また、ＢＳＳ１の最低レベルのセキュリティレベル未満のときには、ステップＳ３３に示すように端末ＷＬ１３の接続を拒否すると判断する。即ち、端末ＷＬ１３の接続を拒否する場合は、例えば、ＩＥＥＥ８０２．１１の規定に従い、ステップＳ３４に示すようにアソシエーションの応答フレーム（Ａｓｓｏｃｉａｔｉｏｎ　ＲｅｓｐｏｎｓｅのＳｔａｔｕｓ　ｃｏｄｅ）に、接続が失敗である旨のコードを書き込んで、端末ＷＬ１３に返信する。端末ＷＬ１３は、このフレームを受信することにより、基地局ＡＰ１から接続を拒否されたと判断して、この段階で接続手続きを中断する。

【０１０４】

一方、端末ＷＬ１３の接続を許可する場合は、端末ＷＬ１３から通知されたＢＳＳ１の最低レベルのセキュリティレベルである”ｅｎｃ．　１”を利用する通信のために、ＩＥＥＥ８０２．１１の規定に従い、アソシエーションの応答フレーム（Ａｓｓｏｃｉａｔｉｏｎ　ＲｅｓｐｏｓｅのＳｔａｔｕｓ　ｃｏｄｅ）に、接続が成功である旨のコードを書き込み、ステップＳ３６に示すように端末ＷＬ１３に返信する。

【０１０５】

これを受けて、端末ＷＬ１３では、ＩＥＥＥ８０２．１１の規定に従い、暗号パラメータを端末ＷＬ１３と基地局ＡＰ１との間で共有するための認証処理の為にステップＳ３７に示すようにオーセンティケーションフレームの送信する。オーセンティケーションフレームの送信後のオーセンティケーションの処理は、ＩＥＥＥ８０２．１１の規定に従って実行される。この処理に関しては、ＩＥＥＥ８０２．１１の規定に従うことから、その説明は省略する。

【０１０６】

尚、この第３の実施形態の場合も、第１の実施形態の場合と同様な効果が期待できるとともに、第１の実施形態で説明したような数々のバリエーションが適用可能であることは云うまでもない。

【０１０７】

（第４の実施形態）

次に、ある端末が複数の基地局のエリア間を移動しながら通信する場合において、各エリア、即ち、ＢＳＳ毎のセキュリティレベルを確保する手法について、図１に示した無線ＬＡＮシステムを例にとり説明する。端末ＷＬが移動される状況、即ち、いわゆるモバイル環境下にお

いても、各基地局の属するＢＳＳに対して夫々に予め定められた最低限のセキュリティレベルを確保するための手法を、この第４の実施形態において説明する。基本的には、上記第１の実施形態で説明したように、各ＢＳＳの基地局では、端末からの接続要求を受ける際に、当該端末からセキュリティレベルを通知してもらい、それが自ＢＳＳに予め定められた最低限のセキュリティレベル以上である場合のみ、当該端末の接続を許可し、基地局と端末との間で暗号パラメータを共有するための認証処理を実行する点は同じである。

【０１０８】

例えば、ＩＥＥＥ８０２．１１に規定されている無線ＬＡＮシステムでは、図１の端末ＷＬ１３が基地局ＡＰ２に接続していたところ、基地局ＡＰ１のエリア内に移動してきた場合には、端末ＷＬ１３と基地局ＡＰ１との間ではリアソシエーション（Ｒｅａｓｓｏｃｉａｔｉｏｎ）が実行される。そして、このリアソシエーション手続きが正常に終了すると、データフレームが送受信される。

【０１０９】

この第４の実施形態では、端末ＷＬ１３から基地局ＡＰ１へは、リアソシエーションの要求フレーム（Ｒｅａｓｓｏｃｉａｔｉｏｎ　Ｒｅｑｕｅｓｔ）中の未使用領域を利用して、端末ＷＬ１３のセキュリティレベルが通知される。

【０１１０】

以下、図１に示した無線ＬＡＮシステムにおいて、端末ＷＬ１３が基地局ＡＰ２のエリアから基地局ＡＰ１のエリアに移動し、基地局ＡＰ１に対しリアソシエーションが実施される場合について、図１５に示すフローチャートを参照して説明する。尚、図１５において、図１３と同一部分には同一符号を付してその説明を省略し、異なる手続きについて説明する。

【０１１１】

端末ＷＬ１３は、ステップＳ３１に示すように基地局ＡＰ１から送信されるビーコンフレームを受信した後、基地局ＡＰ１に接続すべく、ステップＳ５１に示すようにリアソシエーションの要求フレームを基地局ＡＰ１に送信する。

【０１１２】

ＩＥＥＥ８０２．１１に規定されているＭＡＣフレームのリアソシエーションのフレームには、図１４（ａ）～（ｃ）に示すように、そのフレームボディの「Ｃａｐａｂｉｌｉｔｙ　ｉｎｆｏｒｍａｔｉｏｎ」内に未使用領域、即ち、リザーブフィールドが用意されている。

【０１１３】

端末ＷＬ１３の送信部１０７は、ステップＳ５１に示すようにこのリザーブフィールドに端末ＷＬ１３のサポートしているセキュリティレベルのうちの少なくとも所望の１つを書き込み、基地局ＡＰ１に送信する。例えば、ここでは、端末ＷＬ１３の送信部１０７では、自身のもつ全てのセキュリティレベル（"ｅｎｃ．　０""ｅｎｃ．１"）のうち、"ｅｎｃ．１"を示すデータを書き込み、基地局ＡＰ１に送信する。

【０１１４】

このリアソシエーションのフレームを受信した基地局ＡＰ１の処理動作は、図１３の説明と同様であるので、図１３のステップＳ３３に関する説明を参照されたい。但し、ステップＳ３３にて端末ＷＬ１３の接続を拒否する場合は、ＩＥＥＥ８０２．１１の規定に従い、リアソシエーション応答フレームのステータスコードに、接続が失敗である旨のコードが書き込まれ、ステップＳ５２に示すように端末ＷＬ１３に返信される。また、端末ＷＬ１３の接続を許可する場合は、ＩＥＥＥ８０２．１１の規定に従い、リアソシエーション応答フレームのステータスコードに、接続が成功である旨のコードが書き込まれ、ステップＳ５３に示すように端末ＷＬ１３に返信される。

【０１１５】

基地局ＡＰ１が端末ＷＬ１３の接続を許可した場合、基地局ＡＰ１と、端末ＷＬ１３との間で、暗号パラメータが共有されることが必要とされる。そのために、図１５のステップＳ３７～ステップＳ４４に示したように、図１３と同様に、ＩＥＥＥ８０２．１１の規定に従い、暗号パラメータを端末ＷＬ１３と基地局ＡＰ１との間で共有するための認証処理、即ち、オーセンティケーションの手続きが執られても良い。

【０１１６】

また、端末ＷＬ１３からのリアソシエーションの要求フレームには、端末ＷＬ１３が現在接続している基地局、即ち、基地局ＡＰ２のアドレスが記述されている。このアドレスは、図１４（ａ）～（ｃ）に示される「現在のＡＰアドレス（Ｃｕｒｒｅｎｔ　ＡＰ　ａｄｄｒｅｓｓ）」が相当する。そこで、図１５に示したように、オーセンティケーションの手続きが執られず、「現在のＡＰアドレス（Ｃｕｒｒｅｎｔ　ＡＰ　ａｄｄｒｅｓｓ）」を基に、基地局ＡＰ１は、基地局ＡＰ２に接続する。そして、基地局ＡＰ１は、基地局ＡＰ２のセキュリティテーブルに登録されている端末ＷＬ１３についてのセキュリティ情報の転送を要求し、そのセキュリティ情報の転送後に、セキュリティ情報をそのセキュリティテーブルに登録するようにしても良い。これにより、基地局ＡＰ１と端末ＷＬ１３との間で、暗号パラメータの共有される。従って、端末ＷＬ１３がステップＳ５３で示される基地局ＡＰ１から接続が許可された後に、端末ＷＬ１３は、この端末ＷＬ１３と基地局ＡＰ２との間の通信と同様にして、同一のセキュリティレベルで暗号化されたデータフレームを基地局ＡＰ１との間で送受信することができる。

【０１１７】

尚、この第４の実施形態に係る通信システムにおいても、第１の実施形態におけると同様な効果が期待できるとともに、第１の実施形態で説明したような数々のバリエーションが適用可能であることは云うまでもない。

【０１１８】

（第５の実施形態）

以上、第１～第４の実施形態に係る通信システムにおいては、端末ＷＬ１３が基地局ＡＰ１との間で、基地局ＡＰ１の属するＢＳＳ１に予め定められた最低レベル以上のセキュリティレベルにて通信を実現することが可能となる。しかし、端末ＷＬ１３が基地局ＡＰ１と通信すると同時に、端末ＷＬ１３が基地局ＡＰ１以外のＢＳＳ１に加入していない端末や他の無線局と通信する場合に、その間の通信のセキュリティレベルがＢＳＳ１に予め定められた最低レベルより低ければ、結果として、ＢＳＳ１の最低レベルのセキュリティレベルが確保されたとは云えない。そこで、この第５の実施形態に係る通信システムにおいては、端末ＷＬ１３が図１６に示すように、ある端末ＷＬ１４と既に無線接続している場合に、端末ＷＬ１３が基地局ＡＰ１に接続要求したとしても、下記に説明する手続きに従って、ＢＳＳ１に予め定められた最低レベルのセキュリティを確保することができる。

【０１１９】

端末ＷＬ１３は、ＢＳＳ１に予め定められた最低のセキュリティレベルに満たないセキュリティレベルにて、他の端末や基地局に無線接続されている際には、端末ＷＬ１３は、ＢＳＳ１内の基地局或いは端末には接続できないようにすることが基本である。従って、ＢＳＳ１内の端末や基地局に接続するには、予め、このようなセキュリティレベルの低い無線接続を切断しておくか、或いは、その無線接続のキュリティレベルをＢＳＳ１の最低レベル以上に上げることが必要とされる。

【０１２０】

以下、そのための手順を、第１～第４の実施形態で説明した共通の手順については説明を省略し、異なる手順について説明する。

【０１２１】

図１６において、図１と同一部分には同一符号を付してその説明を省略する。図１６に示した端末ＷＬ１４のサポートしているセキュリティレベルは”ｅｎｃ．０”のみであるとする。端末ＷＬ１３が基地局ＡＰ１に接続の要求を開始する際には、端末ＷＬ１３は、既に端末ＷＬ１４に無線接続され、その間の通信セキュリティレベルは”ｅｎｃ．０”であると仮定する。

【０１２２】

このような状態において、端末ＷＬ１３がＢＳＳ１の基地局ＡＰ１に接続要求を開始する場合について説明する。

【０１２３】

まず、第２の実施形態で説明したように、ビーコンフレームにて、ＢＳＳ１に予め定められた最低のセキュリティレベルが通知される場合について、図１７に示したフローチャートを参照して説明する。この場合、端末ＷＬ１３は、受信したビーコンフレームから基地局ＡＰ１に無線接続できる最低のセキュリティレベルが”ｅｎｃ．１”であることを知る。そこで、端末ＷＬ１３は、図１３のステップＳ３２へ進む前に、図１７に示す処理動作を実行する。

【０１２４】

図１７のステップＳ６１において、端末ＷＬ１３のセキュリティレベルに、ＢＳＳ１で許容される最低レベル”ｅｎｃ．１”以上のセキュリティレベルが用意されているかが確認される。”ｅｎｃ．１”以上のセキュリティレベルが端末ＷＬ１３に用意されているときには、ステップＳ６２へ進む。このステップＳ６２において、現在端末ＷＬ１３が無線接続されている端末、即ち、端末ＷＬ１４と端末ＷＬ１３との間の通信のセキュリティレベルがＢＳＳ１で許容される最低レベル”ｅｎｃ．１”以上であるか否かがチェックされる。端末ＷＬ１３と端末ＷＬ１４との間の通信のセキュリティレベルがＢＳＳ１で許容される最低レベル”ｅｎｃ．１”以上であれば、ステップＳ６４へ進み、端末ＷＬ１３と基地局ＡＰ１との間の接続手順が開始される。即ち、端末ＷＬ１３においては、図１３のステップＳ３２以降の処理が実行される。一方、端末ＷＬ１３と端末ＷＬ１４との間のセキュリティレベルがＢＳＳ１で許容される最低レベル（”ｅｎｃ．１”）に満たないときは、ステップＳ６３へ進み、端末ＷＬ１３と端末ＷＬ１４との間の無線接続が切断されて、ステップＳ６４へ進む。

【０１２５】

上述したように、端末ＷＬ１３と端末ＷＬ１４との間の通信のセキュリティレベルは”ｅｎｃ．０”であるから、ステップＳ６２からステップＳ６３へ進み、端末ＷＬ１３と端末ＷＬ１４との間の無線接続が切断される。その後、端末ＷＬ１３は、ＩＥＥＥ８０２．１１に規定されているディオーセンティケーション（Ｄｅａｕｔｈｅｎｔｉｃａｔｉｏｎ）が終了されてステップＳ６４へ進む。

【０１２６】

このように、端末ＷＬ１３は、現在接続している端末ＷＬ１４との間のセキュリティレベルが接続要求される基地局ＡＰ１からブロードキャストされたセキュリティレベルより低いときには、予め端末ＷＬ１３と端末ＷＬ１４との無線接続が切断され、端末ＷＬ１３から基地局ＡＰ１に接続要求がされる。従って、ＢＳＳ１の最低限のセキュリティレベルを保持しながら、端末ＷＬ１３と基地局ＡＰ１との間の無線接続が確実に実行される。

【０１２７】

尚、ステップＳ６３では、端末ＷＬ１３と端末ＷＬ１４との無線接続を一旦切断した後、端末ＷＬ１３と端末Ｗ

ＷＬ１４とは、再度ＢＳＳ１の最低レベル以上のセキュリティレベルで無線接続されても良い。

【０１２８】

上述した説明では、端末ＷＬ１３が端末ＷＬ１４の１つのみと無線接続される場合について説明したが、端末ＷＬ１３が複数の端末或いは複数の基地局に無線接続されている場合も、上記同様にして、その１つ１つのセキュリティレベルがチェックされる。そのセキュリティレベルがＢＳＳ１の最低レベル以上でなければ端末ＷＬ１３と他の端末との接続が一旦切断され、端末ＷＬ１３がセキュリティレベルをＢＳＳ１の最低レベル以上に設定され、基地局ＡＰ１への接続を開始しても良い。

【０１２９】

尚、上記説明では、端末ＷＬ１４と無線接続している端末ＷＬ１３の場合を例にとり説明したが、ＢＳＳ１とは異なる他のＢＳＳ２の基地局ＡＰ２の処理動作にも上記一連の手続きを適用することができる。このように、接続要求を発した側及び接続要求を受けた側が共に、端末ではなく基地局であるときには、複数のＢＳＳにおいて夫々最低限のセキュリティレベルの確保されたＤＳ通信が可能となる。接続要求を発した側が基地局であるとき、当該基地局には複数の端末や基地局と無線接続している場合もあり、このような場合も上記同様にして、その１つ１つのセキュリティレベルをチェックして、これから接続しようとするＢＳＳの最低レベル以上のものでなければアクセスポイントが端末ＷＬ及び他のアクセスポイントとの接続を一旦切断しても良い。その後、必要に応じて、アクセスポイントがこれから接続しようとするＢＳＳの最低レベル以上のセキュリティレベルを設定して、その後、当該所望の基地局への接続を開始するようにすれば良い。

【０１３０】

次に、第１、第３、第４の実施形態で説明したように、オーセンティケーション、アソシエーション、リアソシエーションの際に、端末ＷＬ１３のセキュリティレベルをチェックする場合について、図１８に示したフローチャートを参照して説明する。尚、図１８に示した処理動作は、図７のステップＳ３、図１３及び図１５のステップＳ３３などに対応している。

【０１３１】

端末ＷＬ１３のセキュリティレベルをチェックする場合、前述したように、端末ＷＬ１３は、オーセンティケーションの要求フレーム、或いは、アソシエーションやリアソシエーションの要求フレーム上の未使用領域に、端末ＷＬ１３のセキュリティレベルを書き込むとともに、次に示す①から②のうちの少なくとも１つの項目がその未使用領域或いは他の未使用領域に書き込まれる。

【０１３２】

① 現在端末ＷＬ１３が無線接続されている端末或いは基地局の有無。

【０１３３】

② 端末ＷＬ１３と現在無線接続されている端末或いは基地局との間のセキュリティレベル

ここで、端末ＷＬ１３が複数の端末或いは基地局に無線接続されている場合には、その全てについてのセキュリティレベルが未使用領域に書き込まれる。

【０１３４】

基地局ＡＰ１では、ステップＳ７１に示すようにフレームを受信し、まず、ステップＳ７２に示すように端末ＷＬ１３のセキュリティレベルをチェックする。端末ＷＬ１３のセキュリティレベルがＢＳＳ１に定められている最低のセキュリティレベルを満たさないときは、ステップＳ７３へ進み、接続が拒否される。即ち、第１、第３、第４の実施形態で説明したように、オーセンティケーション、アソシエーションやリアソシエーションのフレームにて、接続拒否が端末ＷＬ１３に通知される。

【０１３５】

一方、端末ＷＬ１３のセキュリティレベルが基地局ＡＰ１のサポートするセキュリティレベルであり、しかもＢＳＳ１に定められている最低のセキュリティレベル以上であるときは、次に、ステップＳ７４へ進む。上記①或いは②の情報から、端末ＷＬ１３に現在無線接続している端末や基地局が存在しないと判断したときは、ステップＳ７５へ進み、端末ＷＬ１３の無線接続が許可される。すなわち、第１、第３、第４の実施形態で説明したように、オーセンティケーション、アソシエーションやリアソシエーションのフレームにて、無線接続の許可が端末ＷＬ１３に通知されるとともに後続の処理が前述したと同様に実行される。この処理には、図７のステップＳ６、図１３のステップＳ３６、図１５のステップＳ５３等が相当する。上記①或いは②の情報から、端末ＷＬ１３に現在無線接続している端末や基地局が存在すると判断したときは、ステップＳ７６へ進む。

【０１３６】

ステップＳ７６において、ステップＳ７１にて受信した情報に、②に示した「端末ＷＬ１３と現在無線接続している端末ＷＬ１４との間のセキュリティレベル」が含まれているときは、そのセキュリティレベルがチェックされる。端末ＷＬ１４との間のセキュリティレベルがＢＳＳ１に定められている最低のセキュリティレベル以上であるときは、ステップＳ７５へ進み、端末ＷＬ１３の無線接続が許可される。一方、端末ＷＬ１４との間のセキュリティレベルがＢＳＳ１に定められている最低のセキュリティレベルに満たないとき、或いは、ステップＳ７１で受信した情報に、上記②に示した情報が含まれていないとき、即ち、端末ＷＬ１４との間のセキュリティレベルが不明なときは、ステップＳ７７へ進み、端末ＷＬ１３からの接続要求が拒否される。第１、第３、第４の実施形態で説明したように、オーセンティケーション、アソシエーションやリアソシエーションのフレームに

37

て、この接続要求の拒否は、端末ＷＬ１３に通知される。

【０１３７】

尚、ステップＳ７７では、接続要求を拒否する旨を通知するのではなく、端末ＷＬ１４との無線接続の切断を指示する旨の要求を、オーセンティケーション、アソシエーションやリアソシエーションのフレームにて、同様にして通知するようにしても良い。この場合、端末ＷＬ１３は端末ＷＬ１４との無線接続を切断すれば基地局ＡＰ１に接続できると直ちに判断することができる。従って、端末ＷＬ１３は端末ＷＬ１４との無線接続を切断した後、例えば、ＩＥＥＥ８０２．１１に規定されているディオーセンティケーション（Ｄｅａｕｔｈｅｎｔｉｃａｔｉｏｎ）を終了した後に、再度、基地局ＡＰ１に接続要求することができる。

【０１３８】

また、ステップＳ７７で、接続要求を拒否した後に、ＩＥＥＥ８０２．１１に規定されているＭＡＣフレームの管理用フレーム、制御用フレームのうち現在未使用のフレーム、例えば、管理用フレームの場合、サブタイプが「０１１０」～「０１１１」などのフレーム、制御用フレームの場合、サブタイプが「００００」～「１００１」などのフレームを利用して、ＢＳＳ１で許容される最低のセキュリティレベルを通知するようにしても良い。ＢＳＳ１で許容される最低のセキュリティレベルの通知がある場合、端末ＷＬ１４が当該最低のセキュリティレベルをサポートできれば、端末ＷＬ１３は、そのセキュリティレベルに接続し直した後、再び、基地局ＡＰ１に接続要求を行うことができる。

【０１３９】

また、上記説明では、端末ＷＬ１３が端末ＷＬ１４の１つのみと無線接続している場合を例にとり説明している。しかし、複数の端末や基地局と無線接続している場合にあっても、上記と同様にして、端末ＷＬ１３は、既に接続している端末や基地局の有無、好ましくは、その１つ１つのセキュリティレベルを通知しても良い。端末ＷＬ１３から既に接続されている無線通信の複数のセキュリティレベルが通知されてきたときには、基地局ＡＰ１は、ステップＳ７６において、その夫々についてのセキュリティレベルをチェックすれば良い。

【０１４０】

上述したように、接続要求を発した側が、既に他の端末や基地局と無線接続している場合であっても、この無線接続のセキュリティレベルが不明なとき、或いは、接続要求を受けた側の最低限のセキュリティレベルに満たないときには、当該接続要求を拒否することにより、接続要求を受けた側の最低限のセキュリティレベルは確保することができる。尚、上記説明は、端末ＷＬ１４と無線接続している端末ＷＬ１３の場合を例にとり説明したが、ＢＳＳ１とは異なる他のＢＳＳ２の基地局ＡＰ２の

38

処理動作としても適用できる。このように、接続要求を発した側及び接続要求を受けた側が共に、端末ではなく基地局であるときには、複数のＢＳＳにおいて夫々の最低限のセキュリティレベルが確保されたＤＳ通信が可能となる。接続要求を発した側が基地局であるとき、当該基地局には複数の端末や基地局と無線接続している場合もある。このような場合も上記同様にして、接続要求を発した側は、既に接続している端末や基地局の有無、好ましくは、その１つ１つのセキュリティレベルを通知することが好ましい。接続要求を受けた側では、接続要求を発した側から、既に接続されている無線通信の複数のセキュリティレベルが通知されてきたときには、ステップＳ７６において、その夫々についてのセキュリティレベルをチェックすれば良い。

【０１４１】

（第６の実施形態）

上記第１の実施形態に係る無線システムにおいては、基地局に接続要求する場合について説明したが、端末から端末への接続要求の場合においても同様の手法を適用することができる。ここでは、図１９に示すように、ＢＳＳ１に属する端末ＷＬ１２に、ＢＳＳ１には加入していない端末ＷＬ１５が接続要求する場合を例にとり説明する。端末ＷＬ１５のサポートできるセキュリティレベルは”ｅｎｃ．　０”のみである。端末ＷＬ１２は、ＢＳＳ１に加入しているため、端末ＷＬ１２が通信する際には、ＢＳＳ１に予め定められた最低限のセキュリティレベルは確保する必要がある。そのために、端末と基地局との間の図７に示したものと同様の処理動作を、端末ＷＬ１２と端末ＷＬ１５との間において実施される。

【０１４２】

図２０は、端末ＷＬ１５から端末ＷＬ１２へ接続要求する場合における、端末ＷＬ１２と端末ＷＬ１５との間の処理手順を示している。尚、図２０において、図７と同一部分には同一符号を付して説明を省略し、以下に異なる点について説明する。

【０１４３】

図２０において、図７に示される基地局での処理動作が端末ＷＬ１２にける処理動作に対応している。従って、ビーコンフレームの送信するステップＳ１は、不要とされている。他のステップＳ２～ステップＳ１２は図７と同様である。尚、アソシエーションの手順は不要とされる。

【０１４４】

図２０に示すように、端末ＷＬ１２と端末ＷＬ１５との間の接続設定の際にも、接続要求を受けた側の端末ＷＬ１２が接続要求を発した側の端末ＷＬ１５のセキュリティレベルをチェックしている。ここで、接続要求を発した側の端末のセキュリティレベルが接続要求を受けた側の装置がサポートするセキュリティレベルであり、しかも、接続要求を受けた側の端末の属するＢＳＳ１の最低

39

のセキュリティレベル以上であれば、端末ＷＬ１５の接続が許可される。接続要求を発した側の端末のセキュリティレベルが接続要求を受けた側の装置がサポートするセキュリティレベルでなく、或いは、接続要求を受けた側の端末の属するＢＳＳ１の最低のセキュリティレベル以下であれば、端末ＷＬ１５の接続が拒否される。接続が許可であれば、当該セキュリティレベルに対応する暗号パラメータを共有するための手処理動作が実行される。

【０１４５】

尚、端末ＷＬ１２が端末ＷＬ１３から接続要求を受けたとき、その端末ＷＬ１２が基地局ＡＰ１と無線接続しているか否かにかかわらず、端末ＷＬ１２は、図２０に示したような処理動作を実行する。

【０１４６】

図１９において、端末ＷＬ１５は、直接データフレームを端末ＷＬ１２へ送信するモードが適用される場合もある。このモードはアドホック（ａｄ　ｈｏｃ）モードと称せられている。このアドホックモードは、オーセンティケーションを経ずに実行することができる。アドホックモードについて、端末ＷＬ１２での処理動作について、図２１に示すフローチャートを参照して説明する。

【０１４７】

端末ＷＬ１２は、ステップＳ８１に示すように端末ＷＬ１５から、基地局を介さずに直接端末ＷＬ１２に宛てたデータフレームを受信する）。このようなデータフレームは、例えば、ＩＥＥＥ８０２．１１の規定によれば、図４に示したＭＡＣフレームのフレームコントロール中の「Ｔｏ　ＤＳ」及び「Ｆｒｏｍ　ＤＳ」が共に「０」であることから容易に判断できる。

【０１４８】

端末ＷＬ１２の受信部１０１では、このデータフレームを受信した際には、ステップＳ８２に示すようにその送信元のアドレスに対応するセキュリティ情報が端末ＷＬ１２のセキュリティテーブル１１０に登録されているか否かがチェックされる。

【０１４９】

端末ＷＬ１５のセキュリティ情報がセキュリティテーブルに登録されているということは、端末ＷＬ１５は、端末ＷＬ１２と当該セキュリティテーブルに登録されているＢＳＳ１に予め定められた最低レベル以上のセキュリティレベルで、過去に通信したことがあるか、そのようなセキュリティレベルで通信することが予め定められていることを意味している。従って、ステップＳ８３へ進み、端末ＷＬ１２は、例えば、ＥＥＥ８０２．１１に規定の、受信したデータフレームに対するＡＣＫフレームを端末ＷＬ１５へ送信し、端末ＷＬ１５との間のデータの送受信を開始する。

【０１５０】

一方、ステップＳ８２において、端末ＷＬ１５のセキュリティ情報がセキュリティテーブルに登録されていないときは、このままでは、端末ＷＬ１５のセキュリティレベルは不明であるから、端末ＷＬ１２は端末ＷＬ１５との間では通信ができない。従って、ステップＳ８４へ進み、上記ＡＣＫフレームは送信せずに、当該端末ＷＬ１５に、オーセンティケーションを要求する旨を通知する。この通知は、ＩＥＥＥ８０２．１１に規定されているＭＡＣフレームの管理用フレーム、制御用フレームのうち現在未使用のフレーム、例えば、管理用フレームの場合、サブタイプが「０１１０」～「０１１１」などのフレーム、制御用フレームの場合、サブタイプが「００００」～「１００１」などのフレームを利用して通知するようにしても良い。

【０１５１】

この通知を受けた端末ＷＬ１５は、図２０に示したステップＳ２以降の処理動作を開始すれば良い。上述したステップ８４において、端末ＷＬ１２は、ＡＣＫフレームを送信し、端末ＷＬ１５がステップＳ２の処理を開始し、その後図２０に示すステップが実行されても良い。

【０１５２】

上記第５の実施形態に係る通信手順では、端末ＷＬ１３が、図１６に示すように、ある端末ＷＬ１４と既に無線接続している場合に、基地局ＡＰ１に対し接続要求した際に、基地局ＡＰ１のＢＳＳ１に予め定められた最低レベルのセキュリティを確保するための手法について説明した。これに対応して、次に、図２２に示すように、端末ＷＬ１５が既にある端末ＷＬ１６と無線接続しているとき、この端末ＷＬ１５が端末ＷＬ１２に接続要求する場合について説明する。

【０１５３】

ここで、端末ＷＬ１６のサポートできるセキュリティレベルは”ｅｎｃ．　０”のみである。端末ＷＬ１２は、ＢＳＳ１に加入しているため、端末ＷＬ１２が通信を開始する際には、ＢＳＳ１に予め定められた最低限のセキュリティレベルは確保する必要がある。そのためには、図１８に示したものと同様の処理動作を、端末ＷＬ１２で実施するようにすれば良い。

【０１５４】

図２３は、端末ＷＬ１５から端末ＷＬ１２へ接続要求する場合の、端末ＷＬ１２と端末ＷＬ１５との間の処理手順を示している。尚、図２３において、図１８と同一部分には同一符号を付してその説明を省略し、異なる部分について説明する。即ち、図２３において、図１８の基地局及び端末ＷＬ１３における処理動作が夫々端末ＷＬ１２及び端末ＷＬ１５における処理動作に対応し、実質的に図１８に示す処理手順と同様の同様の処理が実施される。従って、図２３を参照する説明に関しては、図１８における上記説明中の基地局及び端末ＷＬ１３が夫々端末ＷＬ１２及び端末ＷＬ１５に置き換えれば、特に説明するまでもなく理解可能である。

40

41

【０１５５】
また、図２２において、端末ＷＬ１５がオーセンティケーションを経ずに、直接データフレームを端末ＷＬ１２へ送信しようとする場合も、端末ＷＬ１２は、図２１のフローチャートの処理動作を実施した後に、図２３に示すような処理動作を実施するようにしても良い。好ましくは、端末ＷＬ１２は、図２１のステップＳ８１で、端末ＷＬ１５から、基地局を介さずに直接端末ＷＬ１２に宛てたデータフレームを受信した場合には、すぐに、ステップＳ８４へ進み、当該端末ＷＬ１５に、オーセンティケーションを要求する旨を通知して、必ず、図２３に示した処理動作を実施することが、セキュリティを確保する上で望ましい。端末ＷＬ１５のセキュリティ情報が端末ＷＬ１２のセキュリティテーブルに登録されていることから、端末ＷＬ１５が端末ＷＬ１２以外の端末との無線接続に、端末ＷＬ１２の属するＢＳＳ１の最低限のセキュリティレベル以上で通信するとは限らないからである。

【０１５６】
尚、上記説明では、端末ＷＬ１５が端末ＷＬ１６の１つのみと無線接続している場合を例に説明したが、複数の端末或いは基地局と無線接続している場合も、上記同様にして、端末ＷＬ１５は、既に接続している端末や基地局の有無、好ましくは、その１つ１つのセキュリティレベルを通知する。端末ＷＬ１５から既に接続されている無線通信の複数のセキュリティレベルが通知されてきたときには、端末ＷＬ１２は、ステップＳ７６において、その夫々についてのセキュリティレベルをチェックすれば良い。

【０１５７】
以上説明したように、上記第６の実施形態によれば、複数の端末間の通信においても、そのうちの１つが、最低限守るべきセキュリティレベルが予め定められているＢＳＳ内の端末であるときには、当該セキュリティレベルを確保することができる。

【０１５８】
（第７の実施形態）
上記第１～第６の実施形態では、ＢＳＳのセキュリティレベルを確保する場合について説明した。同様の手法は、ＩＢＳＳにおいて、セキュリティレベルを確保する場合にも適用可能である。

【０１５９】
この第７の実施形態では、図２４に示したような構成のＩＢＳＳ１を例にとり説明する。

【０１６０】
図２４において、ＩＢＳＳ１は、複数の、例えば、３つの端末ＷＬ３１～ＷＬ３３から構成されている。端末ＷＬ３１は、セキュリティレベル”ｅｎｃ．０”、”ｅｎｃ．１”をサポートし、端末ＷＬ３２は、セキュリティレベル”ｅｎｃ．０”、”ｅｎｃ．１”、”ｅｎｃ．２”をサポートし、端末ＷＬ３３は、セキュリティレベル”ｅｎｃ．０”、”ｅｎｃ．１”をサポートするものとする。

42

【０１６１】
ＩＥＥＥ８０２．１１の規定によれば、ＩＢＳＳは、基地局を介さないで、ＩＢＳＳ内の複数の端末間でオーセンティケーションの認証過程を経ずに、直接データフレームを送受信することができる。ＩＢＳＳ１内の各端末がセキュリティテーブルを有し、このセキュリティテーブルにＩＢＳＳ１を構成する各端末のセキュリティ情報を登録して、ＩＢＳＳ１内で予め定められた最低限のセキュリティレベル以上で通信するようにすれば、ＩＢＳＳ１内の端末間では、その最低限のセキュリティレベルは確保できる。

【０１６２】
そこで、ＩＢＳＳ１を構成する複数の端末のうちの１つ、例えば、端末ＷＬ３１に、ＩＢＳＳ１に加入していない、即ち、セキュリティテーブルに登録されていない端末ＷＬ３４から接続要求を受けたときの処理動作について説明する。

【０１６３】
この処理動作も、第６の実施形態と同様に、端末ＷＬ３１は、好ましくは、図２１に示したような処理動作を実施して、受信したデータフレームの送信元のセキュリティ情報が自身のセキュリティテーブルに登録されていないときには、当該データフレームの送信元、即ち、端末ＷＬ３４に対し、オーセンティケーションを要求する旨の通知を送信する。その後、端末ＷＬ３４から、オーセンティケーションのフレームが送信されると、好ましくは、図２３に示すような処理動作が実施される。但し、図２３に示される端末ＷＬ１５は、端末ＷＬ３４に置き換えられれば良い。即ち、端末ＷＬ３４は、オーセンティケーションのフレームに、端末ＷＬ３４のセキュリティレベルを書き込むとともに、上記①から②のうちの少なくとも１つを書き込み、端末ＷＬ３１へ送信する。端末ＷＬ３１は、このようなオーセンティケーションのフレームを端末ＷＬ３４から受信して、図２３に示した端末ＷＬ１２と同様な処理動作が実施されれば良い。

【０１６４】
このようにして、ＩＢＳＳにおいても、そのＩＢＳＳに予め定められた最低限のセキュリティレベルを確保することができる。

【０１６５】
また、複数の端末間の通信においても、そのうちの１つが、最低限守るべきセキュリティレベルが予め定められているＩＢＳＳ内の端末であるときには、当該セキュリティレベルを確保することができる。

【０１６６】
以上の第１～第７の実施形態で説明したように、基地局、端末といった無線ＬＡＮを構成する無線通信装置の

夫々が、少なくとも１つの（好ましくは複数の）セキュリティレベルをもち、下記の（ｘ１）～（ｘ８）に示した特徴を備えることにより、例えば、ＢＳＳやＩＢＳＳといった無線ＬＡＮの基本グループ、即ち、通信グループ毎に予め定められた暗号化による最低限のセキュリティレベルを確保した無線通信が実現できる。また、複数の無線通信装置間の通信において、当該複数の無線通信装置の少なくとも１つが、最低限守るべきセキュリティレベル、換言すれば、最低レベルのセキュリティレベルが予め定められている通信グループ、例えば、ＢＳＳやＩＢＳＳ内の無線通信装置であるときには、必ず上記最低レベル以上のセキュリティレベルは確保することができる。尚、下記（ｘ１）～（ｘ８）のうち、特に基地局である場合と明記されていない特徴に関しては、好ましくは基地局も端末も共通にもつべき機能である。

【０１６７】

（ｘ１）自装置より、他の無線通信装置である第１の無線通信装置に対し接続要求する際、前記第１の無線通信装置に対し、自装置のもつセキュリティレベルのうち該第１の無線通信装置との間の通信で用いるセキュリティレベルである第１のセキュリティレベルを少なくとも１つ通知する。

【０１６８】

（ｘ２）前記第１の無線通信装置に対し接続要求する際、自装置が前記第１の無線通信装置とは別の他の無線通信装置である第２の無線通信装置と既に接続しているときには、該第２の無線通信装置との間の通信で用いているセキュリティレベルである第２のセキュリティレベルを通知する。

【０１６９】

（ｘ３）前記第１の無線通信装置が基地局の場合、該第１の無線通信装置に接続可能な最低レベルのセキュリティレベルがブロードキャストされているときは、自装置のもつセキュリティレベルのうち該最低レベル以上のセキュリティレベルを選択して、それを前記第１の無線通信装置に対し接続要求する際に通知する。

【０１７０】

（ｘ４）前記第１の無線通信装置が基地局の場合、該第１の無線通信装置に接続可能な複数のセキュリティレベルがブロードキャストされているときは、自装置のもつセキュリティレベルのうち、該ブロードキャストされた複数のセキュリティレベルのうちのいずれかに一致するものを選択して、その選択されたセキュリティレベルを前記第１の無線通信装置に対し接続要求する際に通知する。

【０１７１】

（ｘ５）自装置が、他の無線通信装置である第４の無線通信装置から接続要求を受けたとき、Ａ少なくとも、該第４の無線通信装置から通知された該第４の無線通信装置と自装置との間の通信で用いるセキュリティレベルで

ある第３のセキュリティレベルが自装置のもつセキュリティレベルにあり、しかも自装置の属する通信グループ（即ち、例えば、ＢＳＳやＩＢＳＳ）に予め定められた最低レベル以上であるときには、該第４の無線通信装置の接続を許可し、（ｂ）少なくとも、前記第３のセキュリティレベルが該最低レベルに満たないときには、該第４の無線通信装置との接続を拒否する第３の手段を具備する。

【０１７２】

（ｘ５´）前記第３の手段は、Ａ前記第３のセキュリティレベルが、自装置の属する通信グループに予め定められた最低レベル以上であるとともに、前記第４の無線通信装置が前記第４の無線通信装置とは別の他の無線通信装置である第５の無線通信装置と既に接続しているときに、当該第５の無線通信装置との間の通信で用いているセキュリティレベルである第４のセキュリティレベルが前記最低レベル以上であるときには、該第４の無線通信装置との接続を許可し、（ｂ）前記第３のセキュリティレベルが前記最低レベル以上に満たないとき、あるいは、前記第４のセキュリティレベルが前記最低レベルに満たないとき、或いは、前記第４の無線通信装置が前記第５の無線通信装置と既に接続しているときに前記第４のセキュリティレベルが不明であるときには、前記第４の無線通信装置との接続を拒否する。

【０１７３】

（ｘ７）自装置が基地局である場合、自装置の属する通信グループに予め定められた最低レベルのセキュリティレベル或いは、該最低レベル以上の複数のセキュリティレベルをブロードキャストする第４の手段を具備する。

【０１７４】

（ｘ８）前記第４の無線通信装置から複数のセキュリティレベルが通知されてきたとき、その複数のセキュリティレベルに、自装置の属する通信グループに予め定められた最低レベル以上のものがあれば、そのうちの１つを選択して、それを前記第４の無線通信装置へ通知する第５の手段を具備する。

【０１７５】

この発明の実施の形態に記載したこの発明の手法は、コンピュータに実行させることのできるプログラムとして、磁気ディスク（フロッピーディスク、ハードディスクなど）、光ディスク（ＣＤ－ＲＯＭ、ＤＶＤなど）、半導体メモリなどの記録媒体に格納して頒布することもできる。

【０１７６】

【発明の効果】

以上説明したように、本発明によれば、ＢＳＳ、ＩＢＳＳといった、無線ＬＡＮの基本グループ（通信グループ）毎に、それぞれのグループで予め定められた暗号化による最低限のセキュリティレベルを確保した無線通信が行える。また、複数の無線通信装置間の通信におい

て、当該複数の無線通信装置のうちの少なくとも１つが、最低限守るべきセキュリティレベル（最低レベルのセキュリティレベル）が予め定められている通信グループ（例えば、ＢＳＳやＩＢＳＳ）内の無線無線通信装置であるときには、必ず上記最低レベル以上のセキュリティレベルは確
保することができる。

【図面の簡単な説明】

【図１】この発明の実施形態に係る通信システムを概略的に示す模式図である。

【図２】図１に示す基地局の回路構成の一例を示すブロック図である。

【図３】図１に示す無線端末の回路構成の一例を示すブロック図である。

【図４】図１に示す通信システムにおける基地局及び端末との間で転送されるＩＥＥＥ８０２．１１に規定されているＭＡＣフレームの構造を示す模式図である。

【図５】図１に示される通信システムにおける基地局或いは端末が備えるセキュリティテーブルの一具体例を示すテーブルである。

【図６】図１に示される通信システムにおける基地局或いは端末がセキュリティテーブルの他の具体例を示すテーブルである。

【図７】図１に示される通信システムにおける基地局と端末の処理動作の一例を説明するためのフローチャートである。

【図８】（ａ）は、図１に示す通信システムにおける基地局及び端末との間で転送されるＩＥＥＥ８０２．１１に規定されているオーセンティケーションのフレーム構造を示した模式図及び（ｂ）は、（ａ）に示されるフレームの項目に記述される内容を示すテーブルである。

【図９】（ａ）～（ｃ）は、図１に示す通信システムにおける基地局及び端末との間で転送されるＩＥＥＥ８０２．１１に規定されているアソシエーションリクエストフレーム及びアソシエーションリスポンスフレームの構造を示した模式図である。

【図１０】図１に示す通信システムにおける基地局或いは端末が備える更新されたセキュリティテーブルの具体例を示すテーブルである。

【図１１】図１に示される通信システムにおける基地局から端末に向けられるＩＥＥＥ８０２．１１に規定されているビーコンフレームの構造を示す模式図である。

【図１２】図１に示される通信システムにおける基地局から端末に基地局が属するＢＳＳに予め定められた最低レベルのセキュリティレベルが通知されて基地局に接続要求する処理手続きを示すフローチャートである。

【図１３】図１に示す通信システムにおける基地局及び端末との間で転送されるアソシエーション応答フレームを利用してセキュリティレベルが通知され、このセキュリティレベルがチェックされる処理手続きを示すフローチャートである。

【図１４】（ａ）～（ｃ）は、図１に示す通信システムにおける基地局及び端末との間で転送されるＩＥＥＥ８０２．１１に規定されているリアソシエーションリクエストフレーム及びリアソシエーションリスポンスフレームの構造を示した模式図である。

【図１５】図１に示す通信システムにおける基地局及び端末との間で転送されるリアソシエーション応答フレームを利用してセキュリティレベルが通知され、このセキュリティレベルがチェックされる処理手続きを示すフローチャートである。

【図１６】この発明の他の実施形態に係る通信システムを概略的に示すブロック図である。

【図１７】図１６に示される通信システムにおいて、他の無線通信装置に接続されている無線通信装置が更に他の無線通信装置に接続要求する際の接続要求を発した側の処理手続きの一例を説明するためのフローチャートである。

【図１８】図１６に示される通信システムにおいて、他の無線通信装置に接続されている無線通信装置が更に他の無線通信装置に接続要求する際の接続要求を発した側の処理手続きの一例を説明するためのフローチャートである。

【図１９】この発明のさらに他の実施形態に係る通信システムを概略的に示すブロック図である。

【図２０】図１９に示す通信システムにおける端末間で無線接続する為の処理手順を説明するためのフローチャートである。

【図２１】図１９に示す通信システムにおける端末間で無線接続する際の端末での処理動作の一例を説明するためのフローチャートである。

【図２２】この発明のさらに他の実施形態に係る通信システムを概略的に示すブロック図である。

【図２３】図２２に示す通信システムにおける端末間で無線接続する為の端末での処理動作の他の例を説明するためのフローチャートである。

【図２４】この発明のさらに他の実施形態に係る通信システムを概略的に示すブロック図である。

【符号の説明】

ＡＰ１、ＡＰ２…基地局（無線基地局装置）

ＷＬ１１～ＷＬ１６、ＷＬ３１～ＷＬ３４…端末（無線端末装置）

１１…受信機

１２…送信機

１３…受信制御部

１４…送信制御部

２０、１００…アンテナ

２１、１１０…セキュリティテーブル

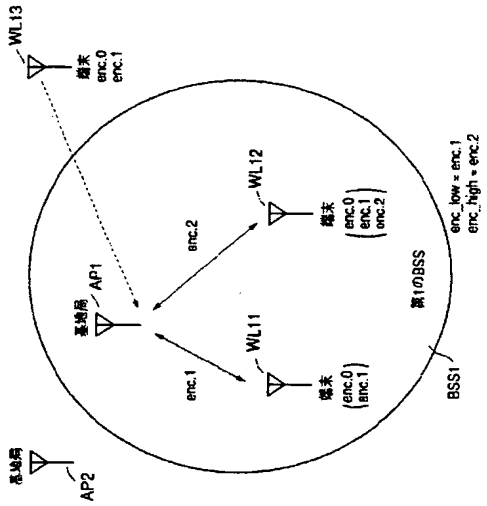
１０１…受信部

１０７…送信部

47

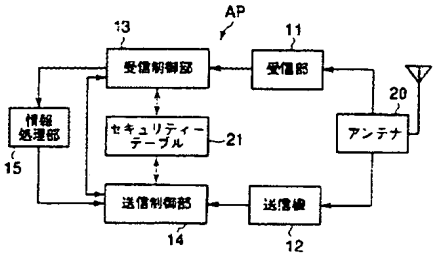
１０８…情報処理部

【図１】

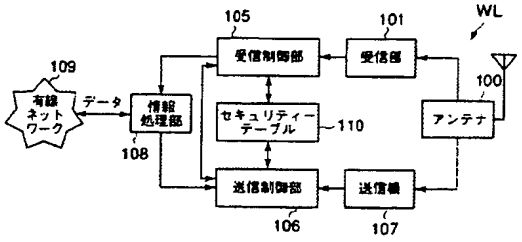


48

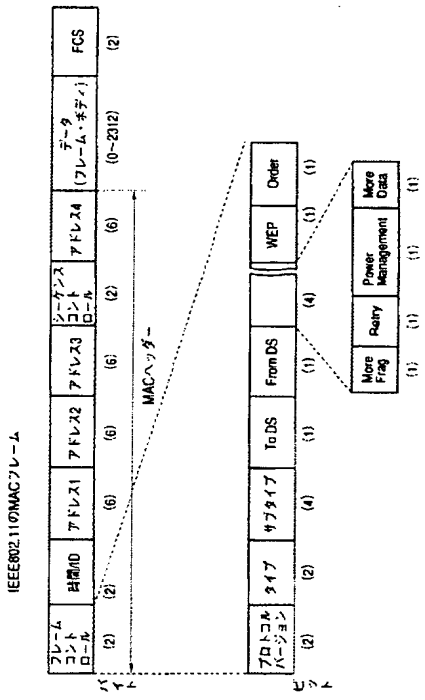
【図２】



【図３】



【図４】



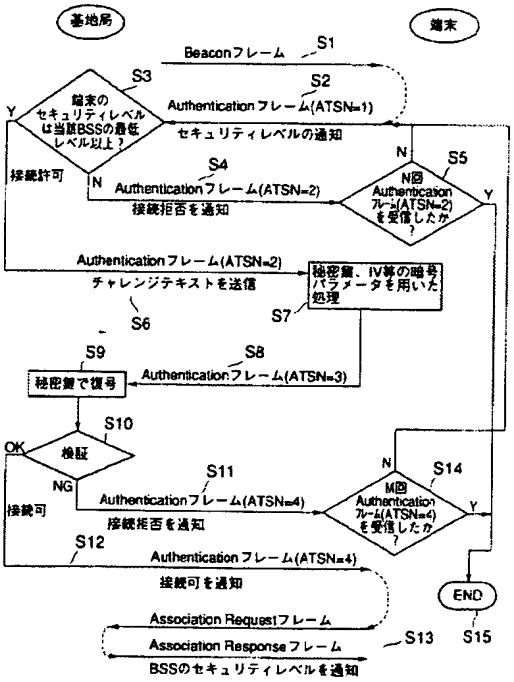
【図５】

	セキュリティレベル	暗号パラメータ	最低レベル
AP1	enc.1 enc.2	key1,IV1 key2,IV2	○
WL11	enc.1	key1,IV1	
WL12	enc.1 enc.2	key1,IV1 key2,IV2	

【図６】

	セキュリティレベル	暗号パラメータ
AP1	enc.1	key1,IV1
WL11	enc.1	key1,IV1
WL12	enc.1 enc.2	key1,IV1 key2,IV2

【図７】



【図８】

(a) Authenticationフレームボディ

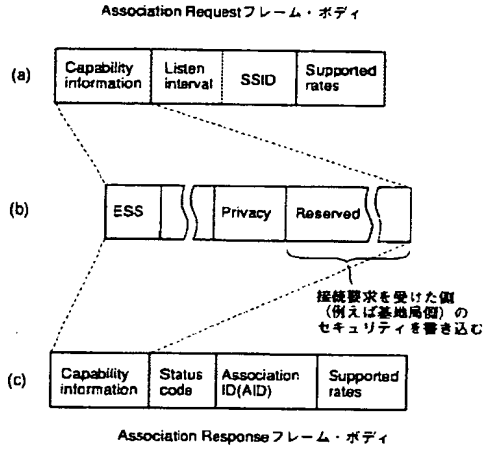
Authentication algorithm number	Authentication transaction number	Status code	Challenge text
	(ATSN)		

(b)

Authentication algorithm	Authentication transaction sequence no.	Status code	Challenge text
Open System	1	Reserved	Not present
Open System	2	Status	Not present
Shared Key	1	Reserved	Not present
Shared Key	2	Status	Present
Shared Key	3	Reserved	Present
Shared Key	4	Status	Not present

※ ATSN=1のStatus codeに接続要求を行った側
(例えば端末側) のセキュリティレベルを書き込む

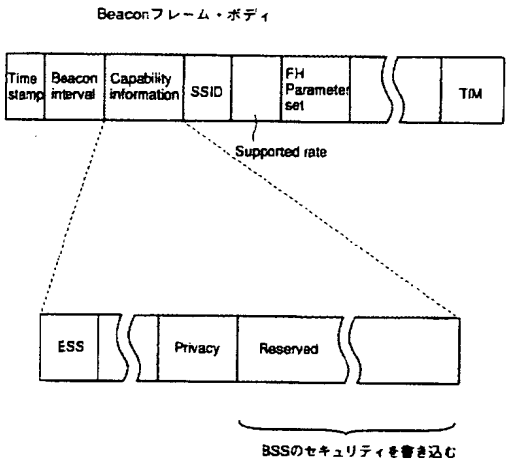
【図９】



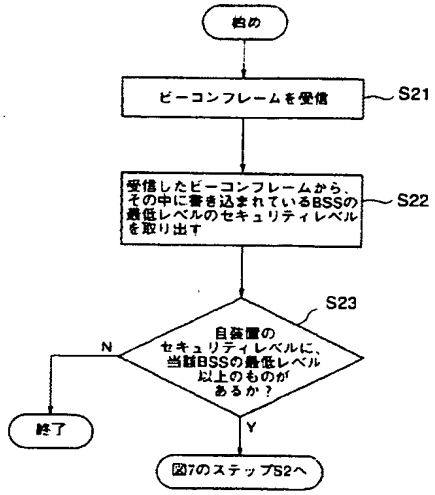
【図１０】

接続先	セキュリティレベル	暗号パラメータ	最低レベル
AP1	enc.1 enc.2	key 1, IV 1 key 2, IV 2	○
WL11	enc.1	key 1, IV 1	
WL12	enc.1 enc.2	key 1, IV 1 key 2, IV 2	
WL13	enc.1	key 1, IV 1	

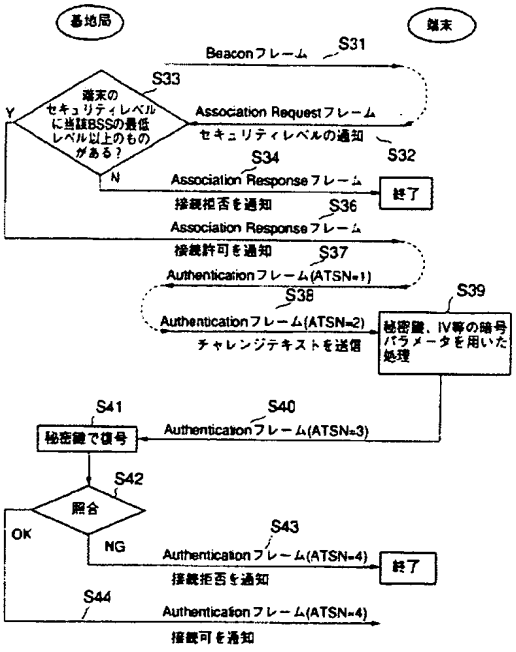
【図１１】


Beaconフレーム・ボディ
Time stamp
Beacon interval
Capability information
SSID
FH Parameter set
TIM
Supported rate
ESS
Privacy
Reserved
BSSのセキュリティを書き込む

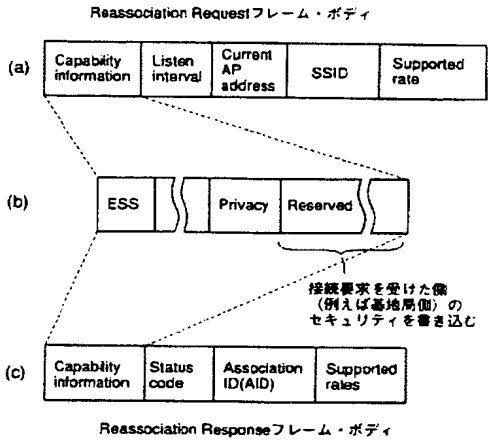
【図１２】


始め
ビーコンフレームを受信
S21
受信したビーコンフレームから、その中に書き込まれているBSSの最低レベルのセキュリティレベルを取り出す
S22
S23
自装置のセキュリティレベルに、当該BSSの最低レベル以上のものがあるか？
N
Y
終了
図7のステップS2へ

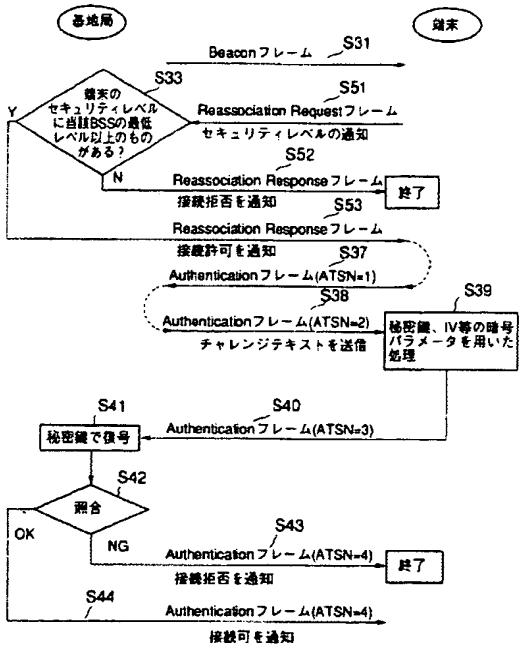
【図１３】


基地局
端末
Beaconフレーム
S31
S33
端末のセキュリティレベルに当該BSSの最低レベル以上のものがある？
Y
Association Requestフレーム
セキュリティレベルの通知
S32
N
S34
Association Responseフレーム
接続拒否を通知
終了
S36
Association Responseフレーム
接続許可を通知
S37
Authenticationフレーム(ATSN=1)
S38
S39
Authenticationフレーム(ATSN=2)
チャレンジテキストを送信
秘密鍵、IV等の暗号パラメータを用いた処理
S41
S40
秘密鍵で復号
Authenticationフレーム(ATSN=3)
S42
照合
OK
NG
S43
Authenticationフレーム(ATSN=4)
接続拒否を通知
終了
S44
Authenticationフレーム(ATSN=4)
接続可を通知

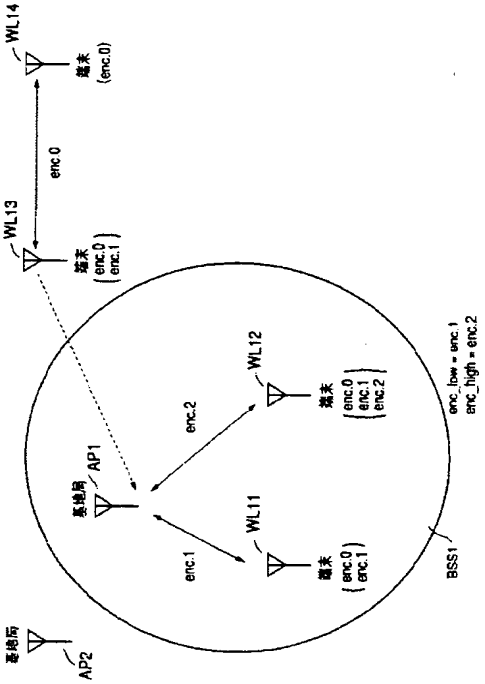
【図１４】


Reassociation Requestフレーム・ボディ
(a)
Capability information
Listen interval
Current AP address
SSID
Supported rate
(b)
ESS
Privacy
Reserved
接続要求を受けた側（例えば基地局側）のセキュリティを書き込む
(c)
Capability information
Status code
Association ID(AID)
Supported rates
Reassociation Responseフレーム・ボディ

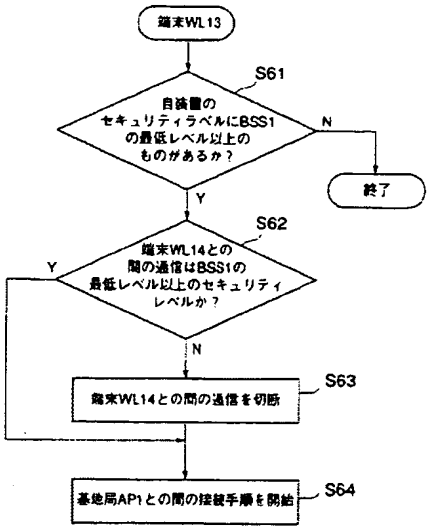
【図１５】


基地局
端末
Beaconフレーム
S31
S33
端末のセキュリティレベルに当該BSSの最低レベル以上のものがある？
Y
N
S51
Reassociation Requestフレーム
セキュリティレベルの通知
S52
Reassociation Responseフレーム
接続拒否を通知
終了
S53
Reassociation Responseフレーム
接続許可を通知
S37
Authenticationフレーム(ATSN=1)
S38
Authenticationフレーム(ATSN=2)
チャレンジテキストを送信
S39
秘密鍵、IV等の暗号パラメータを用いた処理
S41
秘密鍵で復号
S40
Authenticationフレーム(ATSN=3)
S42
照合
OK
NG
S43
Authenticationフレーム(ATSN=4)
接続拒否を通知
終了
S44
Authenticationフレーム(ATSN=4)
接続可を通知

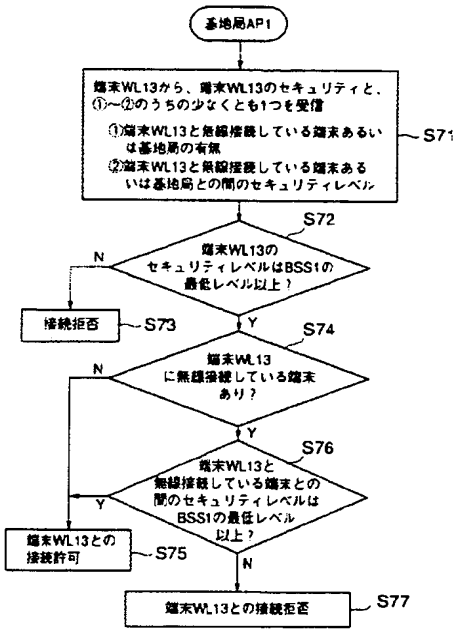
【図１６】


WL14
端末
(enc:0)
enc:0
WL13
端末
(enc:0
enc:1)
WL12
端末
(enc:0
enc:1
enc:2)
enc:2
基地局
AP1
enc:1
WL11
端末
(enc:0
enc:1)
enc_low = enc:1
enc_high = enc:2
BSS1
基地局
AP2

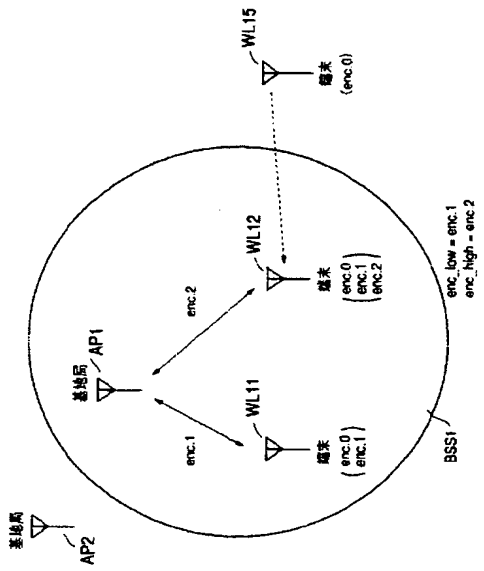
【図１７】


端末WL13
S61
自装置の
セキュリティラベルにBSS1
の最低レベル以上の
ものがあるか？
N
終了
Y
S62
端末WL14との
間の通信はBSS1の
最低レベル以上のセキュリティ
レベルか？
Y
N
S63
端末WL14との間の通信を切断
S64
基地局AP1との間の接続手順を開始

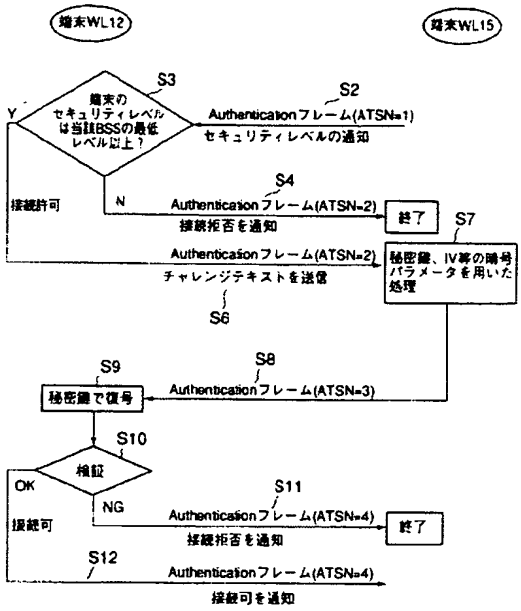
【図１８】


基地局AP1
端末WL13から、端末WL13のセキュリティと、
①～②のうちの少なくとも1つを受信
①端末WL13と無線接続している端末あるい
は基地局の有無
②端末WL13と無線接続している端末ある
いは基地局との間のセキュリティレベル
S71
S72
端末WL13の
セキュリティレベルはBSS1の
最低レベル以上？
N
Y
接続拒否
S73
S74
端末WL13
に無線接続している端末
あり？
N
Y
S76
端末WL13と
無線接続している端末との
間のセキュリティレベルは
BSS1の最低レベル
以上？
Y
N
端末WL13との
接続許可
S75
端末WL13との接続拒否
S77

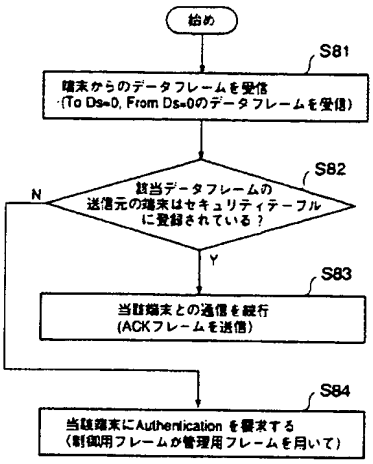
【図１９】


WL15
端末
(enc:0)
WL12
端末
(enc:0
enc:1
enc:2)
enc_low = enc:1
enc_high = enc:2
enc:2
基地局
AP1
WL11
端末
(enc:0
enc:1)
enc:1
BSS1
基地局
AP2

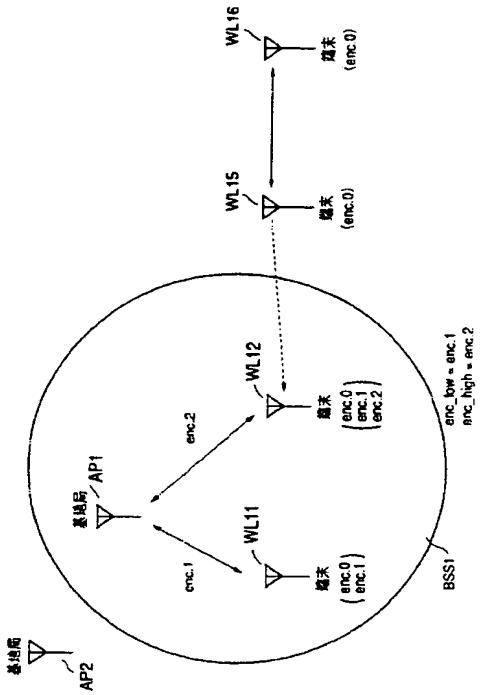
【図２０】


端末WL12
端末WL15
S3
端末の
セキュリティレベル
は当該BSSの最低
レベル以上？
Y
S2
Authenticationフレーム(ATSN=1)
セキュリティレベルの通知
接続許可
N
S4
Authenticationフレーム(ATSN=2)
接続拒否を通知
終了
S7
秘密鍵、IV等の暗号
パラメータを用いた
処理
Authenticationフレーム(ATSN=2)
チャレンジテキストを送信
S6
S9
秘密鍵で復号
S8
Authenticationフレーム(ATSN=3)
S10
検証
OK
NG
S11
Authenticationフレーム(ATSN=4)
接続拒否を通知
接続可
終了
S12
Authenticationフレーム(ATSN=4)
接続可を通知

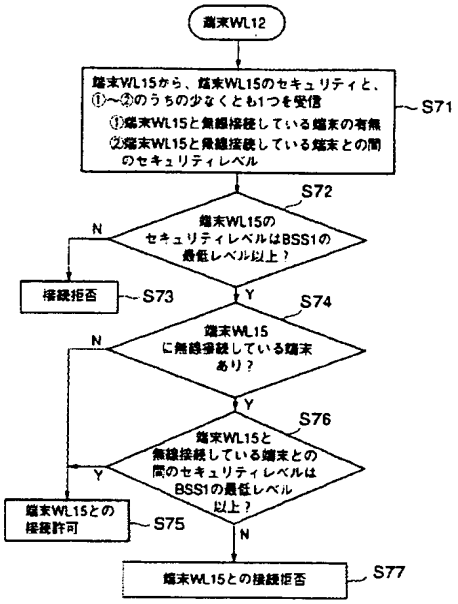
【図２１】


始め
S81
端末からのデータフレームを受信
(To Ds=0, From Ds=0のデータフレームを受信)
S82
該当データフレームの
送信元の端末はセキュリティテーブル
に登録されている？
N
Y
S83
当該端末との通信を続行
(ACKフレームを送信)
S84
当該端末にAuthentication を要求する
(制御用フレームが管理用フレームを用いて)

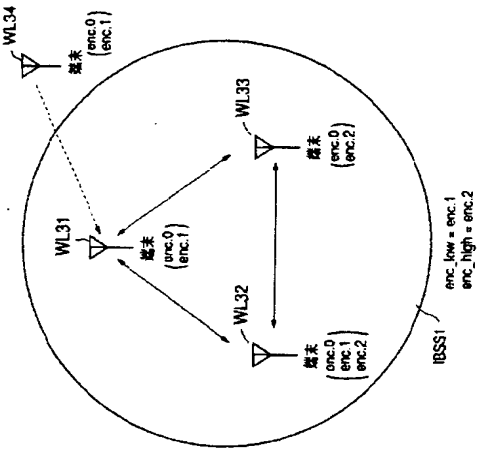
【図２２】


WL16
端末
(enc.0)
WL15
端末
(enc.0)
WL12
端末
(enc.0
enc.1
enc.2)
enc_low = enc.1
enc_high = enc.2
enc.2
基地局
AP1
enc.1
WL11
端末
(enc.0
enc.1)
BSS1
基地局
AP2

【図２３】



【図２４】



フロントページの続き

(74)代理人　100070437
弁理士　河井　将次
(72)発明者　足立　朋子
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(72)発明者　利光　清
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

Ｆターム(参考)　5K033 AA08　CB01　DA01　DA19
5K067 AA30　BB21　CC10　DD04　DD17　EE10　EE12　EE22　HH32　HH36
KK13　KK15

【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成18年6月1日(2006.6.1)

【公開番号】特開2004-32664(P2004-32664A)
【公開日】平成16年1月29日(2004.1.29)
【年通号数】公開・登録公報2004-004
【出願番号】特願2002-378650(P2002-378650)
【国際特許分類】
Ｈ０４Ｌ　12/28　(2006.01)
Ｈ０４Ｑ　7/38　(2006.01)
【Ｆ Ｉ】
Ｈ０４Ｌ　12/28　３００Ｚ
Ｈ０４Ｂ　7/26　１０９Ｒ

【手続補正書】
【提出日】平成18年3月24日(2006.3.24)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
通知セキュリティレベルが記述された第１のフィールドを有する第１の送信フレームを通信グループ外の無線通信装置から受信する受信部と、
非暗号化を含む暗号化方法及び暗号化の強さに依存するセキュリティレベルから選定され、前記無線通信グループに割り当てられた基準セキュリティレベルを記憶するメモリ部と、
前記通知セキュリティレベルを前記基準セキュリティレベルと比較して前記無線通信グループ外の無線通信装置との接続拒否或いは接続許可を決定し、決定された接続拒否或いは接続許可が記載される第２のフィールドを有する第２の送信フレームを発生するフレーム発生部と、及び
この第２の送信フレームを前記無線通信グループ外の無線通信装置に向けて送信する送信部と、
を具備することを特徴とする前記無線通信グループに属する無線通信装置。
【請求項２】
前記基準セキュリティレベルは、第１、第２及び第３のセキュリティレベルから選定され、前記第１のセキュリティレベルが非暗号化に相当し、前記第２のセキュリティレベルが第１の暗号化における第１の暗号化の強さに相当し、前記第３のセキュリティレベルが前記第１の暗号化における第２の暗号化の強さに相当することを特徴とする請求項１の無線通信装置。
【請求項３】
前記フレーム発生部は、前記通知セキュリティレベルが前記基準セキュリティレベルよりも低ければ接続拒否を決定し、前記通知セキュリティレベルが前記基準セキュリティレベルよりも低くなければ接続許可を決定することを特徴とする請求項１の無線通信装置。
【請求項４】
前記接続許可の場合には、前記メモリ部が前記無線通信グループ外の無線通信装置のアドレス及び前記通知セキュリティレベルを保持することを特徴とする請求項１の無線通

信装置。

【請求項５】

前記第２の通信フレームは、前記無線通信グループを特定するアドレスが記述された第３のフィールドを含むことを特徴とする請求項１の無線通信装置。

【請求項６】

無線通信グループに属する第１の無線通信装置及びこの無線通信グループ外の第２の無線通信装置から構成される無線通信システムにおいて、前記第１の無線通信装置は、

通知セキュリティレベルが記述された第１のフィールドを有する第１の送信フレームを前記第２の無線通信装置から受信する受信部と、

非暗号化を含む暗号化方法及び暗号化の強さに依存するセキュリティレベルから選定され、前記無線通信グループに割り当てられた基準セキュリティレベルを記憶する第１のメモリ部と、

前記通知セキュリティレベルを前記基準セキュリティレベルと比較して前記第２の無線通信装置との接続拒否或いは接続許可を決定し、決定された接続拒否或いは接続許可が記載される第２のフィールドを有する第２の送信フレームを発生する第１のフレーム発生部と、及び

この第２の送信フレームを前記第２の無線通信装置に向けて送信する送信部と、

を具備することを特徴とする無線通信システム。

【請求項７】

前記基準セキュリティレベルは、第１、第２及び第３のセキュリティレベルから選定され、前記第１のセキュリティレベルが非暗号化に相当し、前記第２のセキュリティレベルが第１の暗号化における第１の暗号化の強さに相当し、前記第３のセキュリティレベルが前記第１の暗号化における第２の暗号化の強さに相当することを特徴とする請求項６の無線通信システム。

【請求項８】

前記第１のフレーム発生部は、前記通知セキュリティレベルが前記基準セキュリティレベルよりも低ければ接続拒否を決定し、前記通知セキュリティレベルが前記基準セキュリティレベルよりも低くなければ接続許可を決定することを特徴とする請求項６の無線通信システム。

【請求項９】

前記接続許可の場合には、前記第１のメモリ部が前記第２の無線通信装置のアドレス及び前記通知セキュリティレベルを保持することを特徴とする請求項６の無線通信システム。

【請求項１０】

前記第２の通信フレームは、前記無線通信グループを特定するアドレスが記述された第３のフィールドを含むことを特徴とする請求項６の無線通信システム。

【請求項１１】

前記第２の無線通信装置は、前記基準セキュリティレベル及び前記第１の無線通信グループのアドレスを保持する第２のメモリ部を具備することを特徴とする請求項６の無線通信システム。

【請求項１２】

接続拒否が記述される第２のフィールドを有する第２の送信フレームを前記第２の無線通信装置が受信した場合には、前記第２の無線通信装置は、第２の通知セキュリティレベルが記述された第４のフィールドを有する第３の送信フレームを前記第１の無線通信装置に送信することを特徴とする請求項６の無線通信システム。

【請求項１３】

前記第１のメモリは、前記第１の無線通信装置でサポートされるセキュリティレベル及び暗号化レベルに関連する暗号化パラメータを保持し、前記基準セキュリティレベルがこのサポートされているセキュリティレベルから選定されることを特徴とする請求項６の無線通信システム。

【請求項１４】
接続許可が記述される第２のフィールドを有する第２の送信フレームを前記第２の無線通信装置が受信した場合には、前記第２の無線通信装置は、暗号化データが格納されている第５のフィールドを有する第４の送信フレームを前記第１の無線通信装置に送信し、前記第１の無線通信装置が前記暗号化パラメータを用いて暗号化データを複合化することを特徴とする請求項１３の無線通信システム。
【請求項１５】
前記第１の送信フレームは、前記第１の無線通信装置でサポートされている複数の通知セキュリティレベルが記載された第１のフィールドを有し、前記フレーム発生部が前記通知セキュリティレベルの夫々を前記基準セキュリティレベルと比較し、前記通知セキュリティレベルの全てが前記基準セキュリティレベルよりも低ければ接続拒否を決定し、前記通知セキュリティレベルの１つが前記基準セキュリティレベルよりも低くなければ接続許可を決定することを特徴とする請求項１３の無線通信システム。
【請求項１６】
前記通知セキュリティレベルは、前記第２の無線通信装置がサポートする通知セキュリティレベル中の最大のレベルに相当することを特徴とする請求項６の無線通信システム。
【請求項１７】
前記無線通信グループ外の第３の無線通信装置であって前記通知セキュリティレベルで前記第２の無線通信装置と通信している第３の無線通信装置を更に具備することを特徴とする請求項６の無線通信システム。
【請求項１８】
前記無線通信グループに属する第３の無線通信装置であって前記基準セキュリティレベルより低くないセキュリティレベルで前記第２の無線通信装置と通信している第３の無線通信装置を更に具備することを特徴とする請求項６の無線通信システム。
【請求項１９】
前記第１及び第３の無線通信装置の１つは、アクセスポイントに相当することを特徴とする請求項６の無線通信システム。
【請求項２０】
前記第１及び第３の無線通信装置の１つは、無線端末に相当することを特徴とする請求項６の無線通信システム。
【請求項２１】
前記第２及び第３の無線通信装置の１つは、無線端末に相当することを特徴とする請求項６の無線通信システム。
【請求項２２】
前記無線通信グループ外の第３の無線通信装置であって前記通知セキュリティレベルで前記第２の無線通信装置と通信している第３の無線通信装置と、
前記無線通信グループに属する第４の無線通信装置であって前記基準セキュリティレベルより低くないセキュリティレベルで前記第２の無線通信装置と通信している第４の無線通信装置を更に具備することを特徴とする請求項６の無線通信システム。
【請求項２３】
前記第１の無線通信装置がビーコンフレームを第２の無線通信装置に通知して前記第１の送信フレームの送信を要求し、前記ビーコンフレームは、前記第１の無線通信装置でサポートし、前記基準セキュリティレベルより低くないセキュリティーフレームが記載されたフィールドを有することを特徴とする請求項６の無線通信システム。
【請求項２４】
前記第２の無線通信装置は、前記通知セキュリティレベルを含む第２のセキュリティレベルを記憶する第２のメモリ部と、
前記第２のセキュリティレベルを前記基準セキュリティレベルと比較して前記通知セキュリティレベルとして１つのセキュリティレベルを決定して前記第１の送信フレームを発

生する第２のフレーム発生部と、及び
及び
この第１の送信フレームを第１の無線通信装置に向けて送信する送信部と、
を更に具備することを特徴とする請求項６の無線通信システム。
【請求項２５】
通知セキュリティレベルが記述された第１のフィールドを有する第１の送信フレームを通信グループ外から受信し、
非暗号化を含む暗号化方法及び暗号化の強さに依存するセキュリティレベルから選定され、前記無線通信グループに割り当てられた基準セキュリティレベルを記憶し、
前記通知セキュリティレベルを前記基準セキュリティレベルと比較して前記無線通信グループ外の無線通信装置との接続拒否或いは接続許可を決定し、決定された接続拒否或いは接続許可が記載される第２のフィールドを有する第２の送信フレームを発生し、及び
この第２の送信フレームを前記無線通信グループ外の無線通信装置に向けて送信することを特徴とする無線通信方法。
【請求項２６】
第１のフレームコントロールフィールド及びデータフィールドを有する第１のＭＡＣフレームを発生するフレーム発生装置であって、前記フレームコントロールフィールドがタイプフィールド及び暗号化フィールドを含み、当該ＭＡＣフレームが管理フレームに分類される旨が前記タイプフィールドに記述され、暗号化の有無が前記暗号化フィールドに記述され、前記データフィールドが管理データを含み、前記第１のＭＡＣフレームの管理データは、通知セキュリティレベルが記載されたセキュリティレベルフィールドを含むフレーム発生装置と、
前記第１の送信フレームを送信する送信装置と、
を具備することを特徴とする無線通信装置。
【請求項２７】
前記通知セキュリティレベルは、第１、第２及び第３のセキュリティレベルの１つに相当し、前記第１のセキュリティレベルが暗号化なし、前記第２のセキュリティレベルが第１の暗号化方法に基づいて暗号化された第１の強さ備えた第１の暗号化に相当し、前記第３のセキュリティレベルが第２の暗号化方法に基づいて暗号化された第２の強さ備えた第２の暗号化に相当することを特徴とする請求項２６の無線通信装置。
【請求項２８】
前記通知セキュリティレベルは、前記第１の送信装置でサポートされている複数のセキュリティレベル中の最大のものであることを特徴とする請求項２６の無線通信装置。
【請求項２９】
前記無線通信装置は、他の通信装置から第１の送信フレームの送信を要求するビーコンフレームを受信し、このビーコンフレームは、前記基準セキュリティレベルを含むセキュリティレベルが記載されたフレームを含み、このセキュリティレベルは、当該無線通信装置によってサポートされ、前記基準セキュリティレベルよりも高いことを特徴とする請求項２６の無線通信装置。
【請求項３０】
前記他の通信装置は、
前記通知されるセキュリティレベルを含む第２のセキュリティレベルが格納された参照メモリであって、前記第２のセキュリティレベルが暗号化せず及び暗号化強さを含む暗号化方法の１つに依存するセキュリティレベルから選定される第２の参照メモリと、
前記第１のセキュリティレベルを基準セキュリティレベル比較し、１つのセキュリティレベルを通知セキュリティレベルとして決定し、第２の送信フレームを発生する第２のフレーム発生装置と、
前記第２の送信フレームを第１の通信装置に送信する第２の送信装置と、
を具備することを特徴とする請求項２６の無線通信装置。